(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
2010 年 9 月 16 日(16.09.2010)

PCT

(10) 国際公開番号
WO 2010/103628 A1

(51) 国際特許分類:
H04L 9/12 (2006.01)

(21) 国際出願番号: PCT/JP2009/054653

(22) 国際出願日: 2009 年 3 月 11 日(11.03.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社日立製作所 **(HITACHI, LTD.)** [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目６番６号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 戸丸 辰也 **(TOMARU, Tatsuya)** [JP/JP]; 〒3500395 埼玉県比企郡鳩山町赤沼２５２０番地 株式会社日立製作所 基礎研究所内 Saitama (JP).

(74) 代理人: 平木 祐輔 **(HIRAKI, Yusuke)**; 〒1050001 東京都港区虎ノ門４丁目３番２０号 神谷町ＭＴビル１９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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

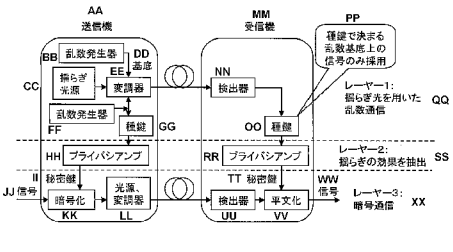
添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) Title: ENCRYPTION COMMUNICATION SYSTEM

(54) 発明の名称 : 暗号通信システム

[図2]

図2



AA TRANSMITTER
BB RANDOM NUMBER GENERATOR
CC FLUCTUATION LIGHT SOURCE
DD BASE
EE MODULATOR
FF RANDOM NUMBER GENERATOR
GG SEED KEY
HH PRIVACY AMPLIFIER
II SECRET KEY
JJ SIGNAL
KK ENCRYPTION
LL LIGHT SOURCE AND MODULATOR
MM RECEIVER
NN DETECTOR
OO SEED KEY
PP EMPLOY ONLY SIGNAL ON RANDOM NUMBER BASE WHICH IS DETERMINED BY SEED KEY
QQ LAYER 1: RANDOM NUMBER COMMUNICATION USING FLUCTUATING LIGHT
RR PRIVACY AMPLIFIER
SS LAYER 2: EXTRACT EFFECT OF FLUCTUATION
TT SECRET KEY
UU DETECTOR
VV DECRYPTION (PLAIN TEXT)
WW SIGNAL
XX LAYER 3: CRYPTION COMMUNICATION

(57) Abstract: Communication having high security against information leakage using an existing optical fiber network is realized. (1) A seed key is shared by a sender and a recipient in advance, and a carrier light having fluctuation is used to transmit and receive a random number using a base determined by the random number. The sender and the recipient each collate a common base defined by the seed key with a random number base, employ only the random number signal superimposed on a matched slot, and share the random number. In this case, although the result of reception involves a bit error because the carrier light has fluctuation, the seed key enables an authorized recipient to receive signals at a bit error rate lower than that of an unauthorized recipient. (2) The quantity of information relating to the random number shared by the sender and the recipient is reduced to a safer quantity by a privacy amplifier, and the random number is used as a secret key. (3) Actual signals are transmitted/received using the obtained secret key.

(57) 要約: 現在の光ファイバ網を利用して、情報漏えいに関して高い安全性を持った通信を実現する。 (1) 送受信者間で予め種鍵を共有し、揺らぎを伴ったキャリア光を用い、乱数で決定される基底を用いて乱数を送受信する。送受信者は種鍵で決まる共有基底と乱数基底を照合し、一致したスロットに重畳された乱数信号のみを採用し、送受信者間で乱数を共有する。この際、キャリア光に揺らぎがあるので受信結果にビット誤りがあるが、種鍵のおかげで正規受信者は不正受信者よりも小さいビット誤り率で受信できる。 (2) 送受信者間で共有された乱数をプライバシアンプにより安全な情報量まで情報量を減らして、それを秘密鍵とする。 (3) 得られた秘密鍵により実際の信号を送受信する。

WO 2010/103628 A1

明 細 書

暗号通信システム

技術分野

[0001] 本発明は光通信システムに関し、特に光通信において安全性を向上させた暗号通信システムに関する。

背景技術

[0002] 通信における秘匿性の要求は古来より未来に亘る永遠のテーマであり、近年のネットワーク社会においては暗号学の発展によりその要求を確保してきた。暗号は共通鍵方式と公開鍵方式に大別できる。共通鍵方式は盗聴されても容易に解読できないことが安全性の根拠であり、公開鍵は解読アルゴリズムが知られているものの解読に非現実的な時間を要することが安全性の根拠である。しかしながら、共通鍵の場合は解読法が発見される可能性があり、また公開鍵の場合も現在知られている解読アルゴリズムよりも高速な解法が発見される可能性があると共に、量子コンピュータが実現すれば現在のアルゴリズムを用いても比較的容易に解読されてしまうため、量子暗号が注目されることになった。

[0003] 量子暗号は量子力学的性質を利用して物理法則的に安全性を保証しようとするものである。通常の暗号が盗聴できても解読が困難であることを安全性の拠り所にしているのに対して、量子暗号は物理法則的に安全性を実現するため、解読法や計算機の進歩があっても安全性が脅かされる心配がない(非特許文献1)。しかし、当然のことながら量子暗号は量子力学的状態を利用するのが条件である。量子力学的状態は環境との相互作用により容易に元の状態から変化する(ディコヒーレンス)ので、量子暗号を現実の通信系に応用する場合は制限事項が多い。光ファイバのような伝送路には必ず損失があり、損失は量子状態を変化させる。従って、量子暗号はまず距離の制限を受ける。例えば100km程度が最大伝送距離である。損失があればその分を補償するため増幅するのが通常の通信であるが、増幅も元の状態をディコヒーレンスさせるので量子暗号では許されない。さらに超微弱光を利用するのが量子暗号の特徴である。こういった性質の量子暗号を運用するためには現在の光通信システ

ムを再構築しなければならない問題もある。以上見たように、量子暗号を運用するには多くの制限事項があることが分かる。

[0004] 以上の量子暗号における課題を解決することを目指して提案されたのがα η スキームと呼ばれる方法で、信号基底を位相空間上で多値にし、隣り合う基底を量子揺らぎの範囲内に設定して盗聴者に正確な情報を与えないようにしたものである(非特許文献2)。このスキームは量子揺らぎを安全性の根拠においているため、信号光強度が大きすぎると量子揺らぎの効果が無視できるようになり、十分な安全性が得られなくなる。量子暗号よりは大きい光強度を利用できるが、通常の光通信における強度に比べれば十分に弱い強度である必要がある。そこで通常の光通信並みの光強度でも適用できるものとして提案されたのがアンチスクイーズを用いた方法である(特許文献1)。多値基底とアンチスクイーズした(広がった)揺らぎを利用して盗聴を困難にしようとするものである。アンチスクイーズした揺らぎは量子揺らぎよりも十分に大きくしたものなので、もはや量子的というよりは古典的揺らぎと言える。

[0005] 通信の安全性を情報理論的に考察した場合は、信号光が量子的であるか古典的であるかを区別しない(非特許文献3, 4)。送信者・正規受信者間の相互情報量I(X;Y)と送信者・不正受信者間の相互情報量I(X;Z)の差により、安全な情報量C=I(X;Y)−I(X;Z)が得られる。相互情報量Iはビット誤り率(BER)の関数で、ビット誤りがない場合には送信者の情報源エントロピーH(A)に一致し、BERの増加と共に減少する。不正受信者のBER(E_E)が正規受信者のBER(E_B)よりも大きければ安全な情報量(C>0)が確保され、情報論的に安全な通信が可能になる。情報論的に安全性を実現するために重要な点は、正規受信者と不正受信者の間に如何に差異を形成し$E_E > E_B$を実現するかにある。量子暗号では量子力学的性質を利用して盗聴された際に正規の送受信者がそれを検知する機能があり、それを利用して$E_E > E_B$を実現する。量子暗号のそれ以外の部分では量子力学的性質は利用しない。従って、量子力学的性質を利用しなくても$E_E > E_B$を実現できる方法があれば安全な通信は可能である。

特許文献1:特開2007−129386号公報

非特許文献1:N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. 74,

145 - 195 (2002).

非特許文献2:G. A. Barbosa, E. Corndorf, P. Kumar and H. P. Yuen, Phys. Rev. Lett. 90 (2003) 227901.

非特許文献3:A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., 54, 1335 (1975).

非特許文献4:U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, 39, 733 (1993).

発明の開示

発明が解決しようとする課題

[0006] 安全性を画期的に向上させるものとして量子暗号が登場したが、現実的に運用するには課題も多く、それを解決するひとつの方法はアンチスクイーズした光のような、古典的な揺らぎを伴ったキャリア光を用いることである。しかしながら、安全な通信を実現するために必要とされる正規受信者と不正受信者間の差異を如何に形成するかは未解決の課題である。本発明では古典揺らぎを利用してこの差異を形成するための方法を開示する。

課題を解決するための手段

[0007] 送受信者間で種鍵を共有することで、正規受信者と不正受信者間に差異を形成する。古典的な揺らぎを伴うキャリア光を用いて、2値の乱数を2基底(一般的にはn及びmを正整数としてn値m基底)で送信する。2つ基底のうちどちらを採用するかも乱数で決定する。理想的に運用した場合、乱数基底の乱数信号なので不正受信者は何の情報も得られない。正規の送受信者は、共有した種鍵を用いて乱数信号を送受信する基底の時系列を共有する(共有基底)。送受信する乱数をすべて信号とみなすのではなく、乱数基底と共有基底を1ビットごとに比較し、一致した場合のみ、そこに重畳された乱数を正規の送受信者間で共有する。正規受信者が乱数基底と共有基底を照合する際にはキャリア光の揺らぎのために判定誤りが発生するが、誤り訂正符号を用いることにより訂正される。正規受信者は基底情報があるので原理的には既知のひとつの基底で2値判定するだけでよいが、不正受信者は基底情報を持たないので2基底で2値判定しなければならない。不正受信者には信号が4値に見えるこ

とになる。4値信号から2値判定した場合のBERは2値信号から2値判定する場合よりも大きくなる。これが正規受信者と不正受信者間の差異である。この差異分に相当する情報量を誤り訂正符号の冗長分で補正し、送受信者間で共有した乱数からプライバシアンプによりその補正した情報量の乱数を生成すれば、安全な秘密鍵が得られる。得られた秘密鍵を用いて実際の信号を暗号通信することにより安全な通信を実現する。

発明の効果

[0008] 本発明は、種鍵を元手に新たな暗号鍵(秘密鍵)を生成している。本方法は種鍵を元手にしているものの、新たに生成された秘密鍵は情報論的に安全性が保証されたものなので、種鍵に対する総当り攻撃以外に有効な攻撃法がないことになる。暗号において種鍵に対する総当り攻撃よりも有効な攻撃法が無い場合、それは十分に安全とみなされる。その意味で本発明は十分に安全な通信システムを実現する。さらに本発明で利用する揺らぎは古典的なものなので、損失及び増幅に対して耐性があり、量子状態を伝送する場合のような伝送距離の制限を受けない。本発明によれば、既存の光ファイバネットワークを利用して、長距離に亘って安全な通信が可能になる。

図面の簡単な説明

[0009] [図1]本発明の物理的原理を示した図である。

[図2]本発明を実現するための原理を示したブロック図である。

[図3]本発明による暗号通信システムの構成例を示したブロック図である。

[図4]図3のブロック図に基づいて本発明を実現した場合の信号例を示す図である。

[図5]位相空間上の信号値を表す領域と揺らぎの関係を示した図である。

[図6]正規受信者と不正受信者のビット誤り率を示すプロットの一例を示す図である。

[図7]本発明による暗号通信システムの構成例を示したブロック図である。

[図8]図7のブロック図に基づいて本発明を実現した場合の信号例示す図である。

[図9]本発明による暗号通信システムの構成例を示したブロック図である。

[図10]図9のブロック図に基づいて本発明を実現した場合の信号例である。

[図11]2値4基底の場合の位相空間上の信号状態を模式的に示す図である。

[図12]4値2基底の場合の位相空間上の信号状態を模式的に示す図である。

[図13]揺らぎ光生成のための構成例を示すブロック図である。

[図14]揺らぎ光生成のための構成例を示すブロック図である。

[図15]レーザーに揺らぎを重畳し、等価的に揺らぎ光源を実現する構成の一例を示すブロック図である。

[図16]変調器に揺らぎを重畳し、等価的に揺らぎ光源を実現する構成の一例を示すブロック図である。

[図17]強度変調方式の場合の各信号の強度分布を示した図である。

符号の説明

[0010] 100 送信機

111～114 乱数発生器

121, 122 種鍵

123, 124 擬似乱数発生器

131～134 バッファ

151 揺らぎ光源

161 変調器

171 プライバシアンプ実行器

181 暗号器

182 光送信機

201, 202 光伝送路

300 受信機

311～313 光検出器

321, 322 種鍵

323, 324 擬似乱数発生器

333, 334 バッファ

341 誤り訂正復号器

371 プライバシアンプ実行器

381 光検出器

382 暗号復号器

1510 レーザー

1520 揺らぎ生成器

1521 光アンプ

1522 帯域透過フィルタ

1523 光ファイバ

1524 サーキュレータ

1525 ファラデーミラー

1530, 1630 揺らぎ発生源

発明を実施するための最良の形態

[0011] 本発明の具体的実施例を記述する前に、まずそのポイントとなる一般的なことを述べる。本発明により通信の安全性を向上させるためには、信号光に揺らぎがあることが重要である。揺らぎがなくてもプロトコルの複雑性が不正受信者の解読困難性を増すが、十分な安全性を得るためには揺らぎが重要である。光の揺らぎは振幅揺らぎと位相揺らぎに大別でき、どちらの揺らぎに対しても本発明は有効であるが、以下の実施例では主に位相揺らぎの場合を例に取って示すことにする。位相揺らぎを利用するので、変調方式は位相変調型である。参照光を必要とするPhase-shift keying (PSK)でも差動型のDifferential-phase-shift keyingでもどちらでも良い。簡単化のため信号は2値、基底数は2とする。この場合、見かけ上信号は4値になる。ただし、本発明は、n及びmを正整数として、n値m基底に容易に拡張することができ、その場合、見かけ上信号はn×m値になる。

[0012] 安全な通信を実現するためには、不正受信者よりも正規受信者が有利な状況を作る必要がある。図1にそれを実現する原理を示す。正規の送受信者は予め種鍵を共有すると仮定し、その種鍵を用いてq軸基底かp軸基底かを決定する。図1(a)はq軸基底の場合の2値信号で、三日月の形は各信号状態“0”及び“1”の位相空間上の揺らぎを表す。信号光の振幅の絶対値をEとすれば、信号“0”は(q, p)＝(E, 0)に、信号“1”は(q, p)＝(－E, 0)に対応するが、キャリア光の揺らぎのために信号光を測定すれば信号“0”の場合は(q, p)＝(E＋δq, δp)に、信号“1”の場合は(q, p)＝(－E＋δq, δp)になる。δqとδpが揺らぎである。図1の三日月はこの揺らぎの

範囲を表し、測定値は概ね揺らぎの範囲内のいずれかの1点になる。図1(b)はp軸基底の場合の2値信号を表す。

[0013] 正規受信者は種鍵により正しい基底で検出でき、原理的には常に図1(c)のような揺らぎの状態で2値判定可能であるが、不正受信者は種鍵を知らないので図1(d)に示すように4値信号に見える。4値信号の揺らぎは隣通しの重なりが大きくなり、不正受信者のBERは増加する。正規受信者にも僅かながらビット誤りが生じるが、不正受信者との差は明らかである。このビット誤り率の差が安全な情報量を確保する。ここで重要な点は、正規受信者が2値信号から2値判定すればよいのに対して不正受信者は4値信号から2値判定しなければならない点である。この差がビット誤り率の差を生成する。但し、単純に同じ鍵を使い続けると不正受信者に基底の推定を許すため、基底の推定を許さないプロトコルを考案することが課題であり、本発明がこれに対する解決法を与える。

[0014] 図2に、本発明による通信プロトコルの全体像を示す。レーヤー1において、揺らぎ光を用いた乱数の送受信をする。安全な情報量は正規受信者と不正受信者のBERの差により決定され、レーヤー2においてはその情報量までプライバシアンプにより乱数データの情報量を縮小して秘密鍵とする(C. H. Bennett, G. Brassard, C. Crepeau, and U. U. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory 41, 1915 (1995).)。レーヤー3は通常の信号伝送路を表し、レーヤー2で得られた秘密鍵を用いて実際の信号を暗号通信する。レーヤー3では揺らぎ光を利用する必要はない。

[0015] レーヤー1では乱数基底で乱数を送受信する。原理的には、レーヤー1の信号は基底も含めて真性乱数のみで構成されるので、不正受信されたとしても何らの情報も漏れない。但し、後述する誤り訂正符号による信号の冗長があるので、これに対する情報量の補正は必要である。正規の送受信者は種鍵により共有基底を予め共有しており、乱数基底で送られてくる乱数信号の中から共有基底に合致したスロットのデータのみを乱数信号として採用する。正規受信者もビット誤りがあるので、以下の具体的実施例で示すように実際の処理はやや複雑になるが、原理的には種鍵のおかげで2値信号を2値判定することになる。不正受信者は4値信号から2値判定しなけ

ればならないため、不正受信者は正規受信者よりも不利なBERで乱数データを受信しなければならない。このBERの差は正規の送受信者に安全な情報量をもたらし、プライバシアンプにより秘密鍵が得られる(レーヤー2)。得られた秘密鍵は、種鍵を使った通信結果から抽出されたものではあるが、正規受信者と不正受信者間のBERに関する差異から抽出したものであり、抽出過程は情報論的なものである。この点が重要である。

[0016] レーヤー3は通常の通信路であり、既知平文攻撃や選択平文攻撃等の各種攻撃にさらされる可能性がある。また、レーヤー1ではビット誤りがあるものの4値信号として不正受信される可能性がある。従って、レーヤー1及びレーヤー3の不正受信結果を照合することにより暗号文が解読される可能性が一見有りうる。しかし、本発明の方法では、正規受信者と不正受信者間のBERに関する差異に基づいて秘密鍵を抽出しているため、レーヤー1とレーヤー3の不正受信結果は情報理論的に無相関になる。レーヤー1は乱数信号のみの送受信なので、暗号文と平文の対応関係のようなデータを不正受信者が得ることはできない。不正受信者が得られるのは、誤り訂正符号の冗長分を除けば真性乱数列のみである。即ち、その冗長分をプライバシアンプにより除去された場合、種鍵に対する総当り攻撃以外に有効な解読法がない。不正受信者が総当り法よりも効率的な攻撃法で解読を実現するためには、少なくともレーヤー1において正規受信者と同じBERで乱数信号を検出できなければならない。この条件が満たされると、レーヤー1とレーヤー3の不正受信結果に相関が出てくる可能性がある。

[0017] 種鍵に対する総当り攻撃以外に有効な攻撃法がないならば、解読法を発見されうるとの脅威から開放され、全数探索(総当り攻撃)に関する計算時間のみで安全性を評価できる。この意味で、本発明の方法は通常の暗号よりも一段階安全性が向上したものである。

[0018] 以下、本発明の実施例について詳細に説明する。

実施例 1

[0019] 基底及び信号の両者を真性乱数化すれば、不正受信者には完全にランダムな信号列だけが見える。図3に本発明による暗号通信システム構成例を示す。送信機10

0内に3台の乱数発生器(111, 112, 113)、乱数からなる2種類の種鍵(121, 122)が配備される。乱数発生器と種鍵は、1台の乱数発生器からの出力を3分割することと、一種類の種鍵を2分割することを行えば、それぞれひとつずつで済ますこともできる。乱数発生器1(111)の出力が秘密鍵生成のための信号となる乱数であり、種鍵2(122)を用いて暗号化され、誤り訂正符号器141により符合化され、バッファ131にて送信される準備をする。バッファ132にはダミー信号用の乱数として乱数発生器2(112)の出力を準備する。乱数発生器3(113)が基底を乱数化するためのもので、この乱数基底に基づいてレーヤー1の信号送信が行われる。正規受信者が正しく受信するためには正規の送受信者間で共有された基底を用いなければならないが、そのために種鍵1(121)を利用する。基底は乱数発生器3(113)により完全にランダムにするが、送受信されたすべての乱数を採用するのではなく、種鍵1(121)で決定される基底に乱数基底が合致した場合のみを採用することとし、不正受信者には乱数に見えるが正規受信者には規則性のある基底の並びに見えるようにする。

[0020] 以上の仕組みで処理される乱数信号及びダミー乱数を具体例で示したのが図4である。基底を指定するのに、図1のq軸基底の場合を“0”、p軸基底の場合を“1”とする。乱数発生器3(113)の出力で決まる乱数基底を、図4に示すように010011101000100とする。一方、送受信者間で予め共有した基底を、1101000011011100とする。図4では共有基底の最初の基底は“1”であるが、乱数発生器3(113)で決まる乱数基底の最初は“0”なので不一致であり、この場合は基底“0”にダミー乱数(バッファ132で待機)を重畳して信号を送信する。信号の重畳は揺らぎ光源151からの出力光に変調器161を通して行う。乱数基底(乱数発生器3(113))の2番目の出力は“1”であり、この場合は共有基底の2番目の出力に一致したので乱数信号(バッファ131に待機)を重畳して送信する。次の共有基底と乱数基底は共に“0”なので引き続き乱数信号を重畳して送信する。以下、同様に繰り返す。

[0021] この方式では、どのタイミングで乱数信号及びダミー乱数を重畳するかは乱数基底(乱数発生器3(113))の出力に依存して決定されるため、図3に示すようにバッファ131とバッファ132を具備して乱数信号及びダミー乱数を待機する。信号(乱数信号及びダミー乱数)が2値、基底も2値であるため、送信する際の信号は4値になる。図

4の「伝送信号」の欄には、左下図のような位相空間上の割り振りをした際の信号値が記されている。「信号」欄の乱数が乱数信号、「ダミー」欄の乱数がダミー乱数である。尚、正規受信者に対して生じるビット誤りを訂正するために乱数データは誤り訂正符号器141により誤り訂正符合化されている。

[0022] 信号(乱数信号及びダミー乱数)は、光伝送路201により伝送され受信機300内の検出器311により受光される。検出器311では4値判定と2値判定を同時に行う。この処理は容易である。2組のホモダイン検出器により2つの直交位相成分(q軸成分及びp軸成分)を測定する。それぞれのホモダイン検出器の出力値I_q, I_pを2値判定(各成分が正か負か)したものが各基底に対する2値判定結果である。2組のホモダイン検出結果の出力値I_q, I_pから$\arctan(I_p/I_q)$により位相φを決定すれば4値判定("0", "1", "2", "3":図4参照)できる。基底が乱数化されているので正規受信者にも信号状態は4値に見える。そこでまずは4値判定することでどちらの基底が利用されたかを判定する。4値判定結果が"0"又は"2"ならば基底"0"、4値判定結果が"1"又は"3"ならば基底"1"と乱数基底の判定をする。これを種鍵1(321)(送信機内の種鍵1(121)と同じもの)で決まる共有基底と照合し、一致すれば重畳されてきた信号を乱数信号と判定し、不一致の場合はダミー乱数と判定する。図4の右側に、以上の受信側の処理の一例を示す。但し、4値判定に基づいて基底の判定を行ったために基底の判定誤り、即ち共有基底との照合判定誤りは多い。

[0023] これを訂正するために、乱数信号に組み込まれた誤り訂正符号のパリティチェック機能を利用する。乱数基底と共有基底の照合に誤りがなければ乱数データのBERは予め推定される小さな値になるが、照合に誤りがあれば誤りがあったビット以降、確率1/2でビット誤りになる。従って、パリティチェックによりビット誤りが始まった位置はほぼ特定できる。このビット誤りが始まった位置は、ダミー乱数が入ってしまったか乱数信号が抜け落ちたかのどちらかである。従って、ビット誤りが始まった位置のビットを抜いてパリティチェックを行うことと、ダミーと判定したために捨てたビットを戻してパリティチェックを行うことを順番に行い、ビット誤りがほぼなくなるビット列を探す。

[0024] ビット誤りがあった場合にどのようになるかの具体例も、図4に示す。簡単化のため、初歩的なパリティチェックのビットを誤り訂正符号器141による誤り訂正符号化におい

て挿入した場合を考える。乱数データを5ビットごとに区切り、“1”の個数が奇数ならば“1”、偶数ならば“0”として、6ビット目にパリティチェックビットとしてその結果を入れたとする。乱数信号は図4の送信側における「信号」欄に示されており、1101010 1である。左から5ビット分のパリティが6ビット目に挿入してある。図4ではパリティビットを斜字体で示す。受信時にビット誤りが無ければ、受信した乱数信号のパリティを計算したものはパリティビットの値と一致する。仮に受信側の乱数基底の判定が、図4の左から6番目のビットで誤ったとする。図4の受信側の例では、下線を付加したビットが判定誤りである。この場合、本来信号ビットでないビットが信号ビットとして扱われることになり、共有乱数が1ビット増えることになる。その結果、パリティチェックビットの位置が1ビットずれる(図4の受信側では、受信者がパリティビットと認識するビットが斜字体になっている。ビット誤りがある場合とない場合で1ビットずれる。)。

[0025] 1ビットずれたことに気付かないで受信者がパリティチェックを行えば、ビット誤りが発生したビット以降、確率1／2でパリティが一致しなくなる。これによりビット誤りがどこで生じたのか概ね判定できる。ビット誤りと思われるビットの乱数基底の判定を変更して受信機の処理を再度行うことを繰り返し、パリティがほぼ正常になるビット列を探す。図4の受信側の例では、下線のあるビットが誤りであり、このビットが共有乱数から削除されることでビット誤りなしの状態に復帰できる。ダミーと判定して一旦捨てたビットを戻す場合は、基底の照合が間違っていた訳だから、戻す際には最初の判定とは異なる基底を基準に信号判定をする。この際の信号判定は、基底が確定しているので2値判定になる。本方式の受信機内の処理は一旦4値判定するが、誤りを訂正する過程で2値判定に還元されることになる。2値判定の場合は、4値判定の場合に比べてBERが小さくなる。これが、正規受信者が不正受信者に対して情報論的に有利になる因子であり、予め送受信者間で共有された種鍵1(121及び321)によりもたらされるものである。

[0026] ビット誤りがほぼ無くなれば、誤り訂正復号器341により誤り訂正符号の復号を行い、種鍵2(322)による復号を行って受信機内で、送信機内の乱数発生器1(111)の出力を再現できたことになる。最終的な秘密鍵生成のためには、1基底2値判定の場合(正規受信者)と2基底2値判定の場合(不正受信者)のBERで決まる情報量差を

誤り訂正符号における冗長分で補正し、プライバシアンプ（171及び371）によりその補正された情報量まで送受信者間で共有された乱数信号の情報量を減らす。

[0027] プライバシアンプは、例えば論理演算を通して実現することができる。送受信者間で共有された乱数の20％が安全な情報量で共有乱数が‘01001 01110’であったとする。5ビットずつ排他的論理和を取ることにすれば‘01’になる。この処理ではすべてのデータを同等に扱い情報量を20％に縮小している。これがプライバシアンプの一例である。

[0028] 正規受信者及び不正受信者のBERは、以下のように見積もることができる。図5に示すように各基底の“0”, “1”の向きを割り振る。信号状態をq軸基底（基底“0”）の信号“0”に取ることにすれば、q軸基底であることを知る正規受信者は測定値がp軸を境界に右側か左側かを判定すればよい。信号“0”に対して正規受信者がq軸の負の領域に測定値を得た場合がビット誤りになる。揺らぎの広がりが量子揺らぎに比べて十分に大きく、測定に関して古典的な取り扱いが可能であるとき、q軸基底の信号“0”の確率分布が位相に関する関数P(θ)で与えられるならば、正規受信者のBERは式（1）で記述される。

[数1]

$$E_B = \int_{-\pi}^{-\pi/2} P(\theta)d\theta + \int_{\pi/2}^{\pi} P(\theta)d\theta \qquad (1)$$

[0029] 不正受信者は、4値に見える信号から2値判定することになり、領域0と領域1に測定値を見出せば信号“0”と判定し、領域2と領域3に測定値を見出せば信号“1”と判定することになるので、信号“0”に対しては領域2と領域3に測定値が見出された場合がビット誤りである。従って不正受信者のBERは式（2）で与えられる。

[数2]

$$E_E = \int_{-\pi}^{-\pi/4} P(\theta)d\theta + \int_{3\pi/4}^{\pi} P(\theta)d\theta \qquad (2)$$

[0030] 揺らぎの確率分布P(θ)が、揺らぎの大きさδθを用いて式（3）により与えられるならば、正規受信者のビット誤り率E_Bと不正受信者のビット誤り率E_Eを具体的に求めることができる。

[数3]

$$P(\theta)=\sqrt{\frac{2}{\pi}}\frac{1}{\delta\theta}\exp\left[-2\left(\frac{\theta}{\delta\theta}\right)^2\right] \qquad (3)$$

[0031] ２δθを変数にしてE_B及びE_Eをプロットしたものが図6である。正規受信者のBERが10^{-12}になるようにガウス分布の揺らぎを設定すれば、不正受信者のBERは10^{-4}程度になる。

[0032] 乱数信号（111）に施される誤り訂正符号（141）は、4値判定（2基底2値判定）した場合の誤りを訂正できる必要はない。受信機における基底の照合過程では、連続的にビット誤りが発生する位置のみを判定できればよい。連続的ビット誤り開始点のビットを特定できれば、そのビットを修正すればBERは2値判定（1基底2値判定）できた場合の予想値にまで下がる。逆に4値判定（2基底2値判定）に対して誤り訂正できてしまうと、正規受信者と不正受信者の揺らぎの効果に基づくBERの差がなくなってしまう。即ち、情報論的に保証された正規受信者と不正受信者間の差異が無くなってしまう。従って、本プロトコルにおいて情報論的に正規受信者と不正受信者の差異を形成するためには、乱数信号に施される誤り訂正符号の能力が1基底2値判定できる正規受信者（例えば、BERが10^{-12}）に対して十分で、2基底2値判定が必要な不正受信者（例えば、BERが10^{-4}）に対して不十分である必要がある。さらに、基底の照合過程で生じた連続的ビット誤り開始点ができるだけ容易に判定できるように誤り訂正符号が設計されていることが望ましい。

[0033] レーヤー1で送受信される信号は乱数であり、基底も真性乱数で決定される。乱数信号は種鍵2（122）により暗号化されるが、信号が乱数なので不正受信者に種鍵2（122）を推定されることはない。共有基底を決定する種鍵1（121）も乱数基底の中に埋もれているので、こちらも不正受信者は推定できない。レーヤー1において不正受信者が意味のある情報を得られないので、正規受信者と不正受信者間に形成されるBERの差が安全な情報量をもたらす。但し、誤り訂正符号の冗長分で補正する必要がある。送信機100内のプライバシアンプ実行器171及び受信機300内のプライバシアンプ実行器371が同じアルゴリズムで演算すれば、送受信機間で共通の秘密鍵が形成される。

[0034] 送信機において生成された秘密鍵を用いて暗号器181により実際の信号を暗号化し、光送信機182によりキャリア光に重畳し、光伝送路202により受信機300まで伝送する。光送信機182は、光源と、その光源の出射光を変調する変調器からなる。

[0035] 受信機300は、伝送された信号光を光検出器381により受光して電気信号に変換し、暗号復号器382により秘密鍵を用いて平文化する。以上で、安全な暗号通信の一連の過程が終了する。

[0036] 光伝送路202で行う通信は、揺らぎを伴うキャリア光を用いる必要は無く、通常の光通信でよい。光伝送路202と201は物理的に異なるものでも良いし、同じ光伝送路を用いて波長多重を行っても良い。

実施例 2

[0037] 実施例1では乱数基底と共有基底を1ビットごとに対にして比較し、乱数信号を送信するかダミー乱数を送信するか決定した。乱数基底の中から共有基底を選ぶ方法は実施例1以外の方法も可能であり、それを実現する暗号通信システムの構成例を示したのが図7である。本実施例は、共有基底と乱数基底を照合して乱数信号とダミー乱数のどちらを送信するかを決定するのは実施例1の方式と同様である。ただし、共有基底と乱数基底が不一致の場合に、不採用になった共有基底を次のビットで再度乱数基底と照合して乱数信号とダミー乱数のどちらを送信するかを決定する点が異なる。共有基底は乱数基底と一致するまで照合を繰り返す。言い換えれば、乱数信号が重畳される基底の並びが共有基底の並びに一致するように運用される。

[0038] 以上の仕組みを具体例で示したのが図8である。乱数発生器3(113)の出力で決まる乱数基底は、図8では0100111010000100である。一方、乱数からなる種鍵1(121, 321)によって送受信者間で予め共有した基底は、10110000である。送信機側においては、まず共有基底で決まる基底の並びで乱数信号を送信する準備をする。図8の例では、共有基底の最初の基底は“1”であるが、乱数発生器3(113)で決まる乱数基底の最初は“0”であり不一致なので、この場合は基底“0”にダミー乱数(乱数発生器2(112)の出力)を重畳して信号を送信する。不一致だった共有基底“1”は、再度次の乱数基底と照合される。乱数基底(乱数発生器3(113))の2番目の出力は“1”であり、この場合は共有基底の最初の基底“1”に一致したので、乱数信

号を重畳して送信する。乱数信号は実施例1と同様に誤り訂正符合化され、簡単化のため実施例1と同様に5ビットごとにパリティビットを加えるものとする。図8の送信側では、パリティビットを斜字体にしている。

[0039] 受信機300側の処理も、送信機100側の処理の変形に基づき実施例1の処理から変形される。まず4値判定を行い、どちらの基底が利用されたかを判定する点は、実施例1の方式と同様である。これを共有基底と照合し、一致すればその乱数データを採用し、不一致の場合はダミー乱数と判定する。不一致だった共有基底は、次に受信信号から判定される乱数基底と再び照合され、一致すればその基底と乱数データとが採用される。パリティチェックによりビット誤りがあった場合、始まった位置がほぼ特定される。このビット誤りが始まった位置は、ダミー乱数が入ってしまったか乱数信号が抜け落ちたかのどちらかなので、ビット誤りが始まった位置付近のビットを抜いてその位置以降の基底照合を再度やり直してパリティチェックを行うことと、ビット誤りが始まった位置付近でダミーと判定したために捨てたビットを戻してその位置以降の基底照合を再度やり直してパリティチェックを行うことを順番に行い、ビット誤りがほぼなくなるビット列を探す。ビット誤りが無かった場合とあった場合の例を、図8の右側に示す。この例では、左から2番目のビットの基底照合が判定誤りになり(受信側に下線で示す)、本来共有乱数となるべき乱数信号をダミー乱数と判定してしまっている。このため採用データのビット数が減り、パリティビットの位置がずれてしまうと共に共有乱数がまったくの別物になってしまう。図8の例では、基底判定誤りがある場合に共有乱数のスロット位置が原型を留めないほど変わっている様子がわかる。この場合、以降のパリティビットは確率1／2で誤りになり、ビット誤りがあった位置が概ねわかることになる。ビット誤りの位置がほぼ特定できれば、その付近のビットを修正し、ビット誤りがほぼなくなるまで修正を繰り返す。

[0040] 実施例2の方式では、受信機において基底判定の誤りに基づいて信号ビットの挿入あるいは除去を行った際に、それ以降の基底照合を再度やり直す必要があるため、実施例1の方式に比べて処理が多くなる欠点があるが、共有基底の並びが種鍵だけで完全に決定される長所がある。

実施例 3

[0041] レーヤー1における乱数の送受信で不正受信者に対して意味のある情報を与えないためには、信号と共に基底も乱数で決定される必要がある。しかしながら、実施例1及び実施例2で見たように正規受信者に対してもビット誤りがあるために乱数基底の中から共有基底を抽出する過程は幾分複雑である。現実的運用の観点からもう少し簡便な方法でこれを実現したい。それを実現するためのシステムの一つが、図9に示した暗号通信システムである。

[0042] 図9に示すプロトコルでは、乱数発生器を3台(111, 112, 114)と乱数からなる種鍵を3個(122, 123, 124)利用する。実施例1と同様に、一台の乱数発生器の出力と1つの種鍵をそれぞれ3分割して使う方法もある。実施例1では乱数信号を送るスロットとダミー乱数を送るスロットの並びは乱数発生器3(113)を用いて真性乱数により決定されたが、本実施例では擬似乱数発生器124により決定する。乱数信号(乱数発生器1(111)の出力)を送信するスロットの基底は擬似乱数発生器123で決まる共有基底を用い、ダミー乱数(乱数発生器2(112)の出力)を送信するスロットの基底は乱数発生器3(114)により決定する。本実施例では、送信信号のどのスロットに乱数信号が埋め込まれているかを種鍵2(擬似乱数発生器124)により予め送受信者間で取り決めておくことになる。送信基底は真性乱数ではなくなっており、安全性に関しては実施例1及び2よりは劣ることになるが、データ処理は容易になる。

[0043] 基底及び乱数信号の処理の具体例を示したのが図10である。擬似乱数発生器123で決まる共有基底が10110000で、乱数発生器3(114)で決まる乱数基底が0010111である。これらの2種類の基底情報の並びを決定するのが擬似乱数発生器124の出力0100111010001O1である(図10左側の「採用スロット」の欄)。“0”の際は共有基底を送信基底とし、“1”の際は乱数基底を送信基底とする。その結果の送信基底が100101011000101になる。不正受信者が見る基底は真性乱数(乱数発生器3(114))と擬似乱数(擬似乱数発生器123)をもうひとつの擬似乱数(擬似乱数発生器124)を使って並べたものであり、擬似乱数発生器123及び124が使われているものの、各信号の基底を解読することは困難である。尚、乱数信号を送信するのかダミー乱数を送信するのかは擬似乱数発生器124により決定され、そのタイミングに合わせて信号送信できるように実施例1及び2と同様にバッファ133及び134が具備

される。本実施例では、乱数信号と共有基底が対をなし、またダミー乱数とダミー基底が対を成しているので、バッファ133及び134ではそれぞれそれらの対で一時待機する。乱数信号（乱数発生器1（111）からの出力）が種鍵3（122）により暗号化される点と誤り訂正符合化（141）される点は、実施例1及び2と同様である。送信信号が見かけ上4値になるのも同様である。

[0044] 受信機では2組のホモダイン検出器312，313を用いてq軸基底（基底“0”）及びp軸基底（基底“1”）に対する射影検出を行い、それぞれ2値判定する。擬似乱数発生器324の出力（擬似乱数発生器124の出力と同じもの）が“0”に相当するスロットの検出結果のみを受信乱数として処理し、ダミースロット（擬似乱数発生器324の出力が“1”）の信号は無視する。乱数信号の基底は擬似乱数発生器323の出力（擬似乱数発生器123の出力と同じもの）で決まっているので、それに従い、2組のホモダイン出力のどちらを採用するかを決定する。

[0045] 共有基底のスロットを決める擬似乱数発生器324の出力は伝送クロックに同期するが、乱数信号は送信されてくる信号の一部なので、共有基底を決定する擬似乱数発生器323の出力はバッファ333で一時待機し乱数信号が来るタイミングに合わせる。擬似乱数発生器323の出力（共有基底）に基づき2つの光検出器312及び313のどちらかの出力を採用し、その出力値（共有乱数）はバッファ334に入力され、出力タイミングが調整されて誤り訂正符号の復号器341に入力される。その後、種鍵3（322）（種鍵3（122）と同じもの）により暗号が復号化され、送信機内の乱数発生器1（111）の出力が再現される。以上により送受信者間で乱数信号を共有できたので、送受信機双方でプライバシアンプ実行器（171及び371）による処理を実施し、秘密鍵を共有する。秘密鍵を用いての実際の信号の暗号通信は実施例1及び2と同様である。

[0046] この方法では採用スロットと採用基底が予め決まっているので、実施例1及び2の真性乱数基底方式の場合のような情報論的安全性を保証できるわけではないが、不正受信者の解読が困難であることに変わりなく、不正受信者による解読が困難で且つ比較的運用が容易なシステムを構築できる。

実施例 4

[0047] 実施例3までは2値2基底の位相変調方式を示した。本発明の方式は一般的には、

n及びmを正整数としてn値m基底で運用可能である。例えば、図11は、2値4基底の位相変調方式の場合の位相空間上の信号状態を示す図である。図11(a)はq軸基底の2値信号を示し、図11(b)はq軸から45°回転した基底の2値信号を示している。また、図11(c)はp軸基底の2値信号を示し、図11(d)はq軸から－45°回転した基底の2値信号を示している。図12は、4値2基底方式の位相変調方式の場合の位相空間上の信号状態を示す図である。図12(a)はq軸及びp軸を基底とする4値信号を示し、図12(b)は図12(a)の場合から45°回転した基底の4値信号を示している。

[0048] ここで、各実施例に共通の要素である揺らぎ光源151について説明する。揺らぎ光源151は様々な形態が考えられるが、光ファイバのカー効果を使った方法が便利である。一例を図13に示す。レーザー光源1510からの出力光は光アンプ1521により増幅され、帯域フィルタ1522を通過して光ファイバ1523を伝播する。この際、光ファイバのカー効果を通して位相揺らぎが加わる。レーザー出力光はコヒーレント状態で比較的よく記述でき、位相空間上の揺らぎの形が円形であるが、光ファイバのカー効果を通して楕円形、またさらに進んで三日月形になる。このように揺らぎの形が楕円形や三日月形になった光をアンチスクイズド光と呼ぶ(T. Tomaru, and M. Ban, "Secure optical communication using antisqueezing," Phys. Rev. A 74, 032312 (2006), T. Tomaru, "LD light antisqueezing through fiber propagation in reflection-type interferometer," Opt. Exp. 15, 11241 (2007))。カー効果は光強度に比例して大きくなるので、パルス光にしてピーク強度を大きくするのが有効である。この場合、ファイバ伝播に伴うパルス広がりを抑えることが効果的であり、ソリトン条件を満足するようにパルス幅、光強度、ファイバの分散値を選ぶと良い(特開2008－003339号公報)。また、上記のソリトン条件よりもさらに光強度を増加させると高次ソリトンの条件を満たすことが可能になり(特開2008－003339号公報)、パルス幅縮小効果が働きカー効果を増強することができる。またその際スペクトル幅が拡大することになり、スペクトルの拡大は位相検出において位相揺らぎと同等な効果を示すので、さらに揺らぎの効果が増強される。またカー効果と同様に、ラマン効果も位相揺らぎの拡大に有効である。

[0049] 図14は、光サーキュレータ1524とファラデーミラー1525を用いてファイバ伝播の部分を往復にした実施例である。ファイバ長を半分にできる点が有利である。また、フ

ァイバ伝播中の偏波状態に係わらずファイバ1523を1往復した時点で偏波がちょうど90度回転するので、揺らぎ生成器出力時の偏波を安定させたい場合に有効である。さらに、揺らぎ生成器1520内にファイバ干渉計を組み、振幅に対する位相揺らぎの比を大きくして、位相揺らぎの効果を大きくすることも有効である(T. Tomaru, "LD light antisqueezing through fiber propagation in reflection-type interferometer," Opt. Exp. 15, 11241 (2007))。

[0050] 以上は、光ファイバのカー効果により位相揺らぎを発生させるものであった。レーザーダイオード(LD)から直接位相揺らぎを伴う光を出力させることも可能である。LDを発振閾値近傍で動作させれば位相揺らぎが大きい。この性質をそのまま利用するのもひとつの方法である。

[0051] LD発振のためには注入電流が必要である。注入電流に揺らぎ(ノイズ)を重畳し、光源自体の揺らぎと同様な効果を発生させることも可能である。図15にその場合を示す。揺らぎ発生源としては、例えば、熱揺らぎを利用することが考えられる。また、揺らぎはアナログ的な乱数と考えることもできるので乱数発生器の出力を多値にして揺らぎと等価的にすることもできる。

[0052] 揺らぎの重畳は、また、変調器161において行うこともできる。変調器161は信号重畳のために設置されているものであるが、信号重畳と共に揺らぎも同時に重畳すれば、光源に揺らぎがある場合と等価な働きをする(図16)。揺らぎ発生源1630としては、熱揺らぎを利用することや、乱数発生器の出力を多値にして揺らぎと等価的にすること等が考えられる。

実施例 5

[0053] これまでは位相変調方式を例にとって示してきた。しかし、本発明は強度変調方式においても適用可能である。図17に、2値2基底で運用する場合の強度分布関数の様子を示す。強度変調方式では"0", "1"の信号強度が基底に依存して変化する。図17(a)と図17(b)は、それぞれ基底が異なる場合の2値の信号である。基底の違いに起因して、"0"と"1"の閾値が図17(a)と図17(b)では異なる。基底を知らない場合、図17(d)に示すように、信号状態は合計4値になり、4値判定が必要になる。確率分布には重なりがあるためにビット誤りが多くなる。基底を知る正規受信者は、実

施例1及び2のように判定過程において一旦4値判定をする場合もあるが、原理的に2値判定可能なので、図17(c)に示すように、確率分布の重なりがほとんど無い状態で2値判定できる。

[0054] 2値判定及び4値判定する点は、位相変調方式の場合も強度変調方式の場合も同様である。従って、実施例1～3に示した位相変調方式に対する信号処理は、強度変調方式の場合に対しても同様に実施することができる。

[0055] 以上、位相変調方式を主な例に取って本発明の実施例を説明した。しかし、実施例5で言及したように、本発明は位相変調方式及び強度変調方式の区別無く成立するものである。また、主に2値2基底を例にとって実施例を述べたが、図11、図12を用いて説明したように、さらに多値多基底の場合でも本発明を適用することができる。

産業上の利用可能性

[0056] 本発明では種鍵を元手に揺らぎを利用して安全な秘密鍵を生成できることを示した。本発明は種鍵を元手にしているものの、秘密鍵生成の過程は情報論的に安全性が保証されたものである。従って、不正受信者が暗号文の解読を試みようとしても、種鍵に対する総当り攻撃以外に有効な攻撃法がないことになる。即ち、暗号文の効率的な解読法が発見されるかもしれないとの脅威から開放されることになる。本発明による方式は、現在の光通信ネットワークをそのまま利用することが可能であり、現実的で適用性の高い方式である。これら2つの理由から本発明は産業上、利用可能性が高い。

請求の範囲

[1] 第1の乱数発生器、誤り訂正符号器、第2の乱数発生器、第3の乱数発生器、第1の光源、第1の変調器、プライバシアンプ、暗号器、並びに第2の光源及び第2の変調器を有する光送信機を具備する送信機と、

第1の光検出器、誤り訂正復号器、プライバシアンプ、第2の光検出器、及び暗号復号器を具備する受信機と、

前記送信機と前記受信機をつなぐ光伝送路とを有し、

前記送信機と前記受信機は予め乱数からなる第1の種鍵を共有し、前記第1の種鍵は前記送信機と前記受信機に共有基底を与え、

前記送信機は、前記第1の乱数発生器の出力を乱数信号として前記誤り訂正符号器によって誤り訂正符合化し、

前記第2の乱数発生器の出力をダミー乱数とし、前記第3の乱数発生器の出力を前記乱数信号及び前記ダミー乱数送信のための乱数基底とし、前記乱数基底と前記共有基底が一致した場合には前記乱数信号を信号とし、前記乱数基底と前記共有基底が一致しない場合には前記ダミー乱数を信号とし、

前記第1の光源からの出力光に前記第1の変調器により、前記乱数基底で前記信号を重畳して第1の信号光とし、

その際、前記第1の光源からの出力光は揺らぎを伴うか、あるいは前記第1の光源又は前記第1の変調器において揺らぎが重畳され、

前記第1の信号光は前記光伝送路に出力され、

前記プライバシアンプは前記第1の乱数発生器の出力である乱数信号のビット数を減らして秘密鍵を生成し、

前記暗号器は前記秘密鍵を用いて送信信号を暗号化し、

前記光送信機から前記暗号化した送信信号によって変調した第2の信号光を出力し、

前記受信機は、前記第1の光検出器で前記第1の信号光を受信し、

乱数基底及び信号の値を判定し、受信した乱数基底と前記共有基底とを照合し、一致した場合の信号を誤り訂正符号化された乱数信号として、前記誤り訂正復号器

で復号し、

前記プライバシアンプによってビット数を減らして秘密鍵を取り出し、

前記第2の光検出器で前記第2の信号光を受信し、

前記取り出した秘密鍵を用いて前記暗号復号器で、前記第2の光検出器で受信した信号から前記送信信号を復号することを特徴とする暗号通信システム。

[2] 第1の乱数発生器、誤り訂正符号器、第2の乱数発生器、第3の乱数発生器、第1の光源、第1の変調器、プライバシアンプ、暗号器、並びに第2の光源及び第2の変調器を有する光送信機を具備する送信機と、

第1の光検出器、誤り訂正復号器、プライバシアンプ、第2の光検出器、及び暗号復号器を具備する受信機と、

前記送信機と前記受信機をつなぐ光伝送路とを有し、

前記送信機と前記受信機は予め乱数からなる第1の種鍵を共有し、前記第1の種鍵は前記送信機と前記受信機に共有基底を与え、

前記送信機は、前記第1の乱数発生器の出力を乱数信号として前記誤り訂正符号器によって誤り訂正符合化し、

前記第2の乱数発生器の出力をダミー乱数とし、前記第3の乱数発生器の出力を前記乱数信号及び前記ダミー乱数送信のための乱数基底とし、

前記乱数基底と前記共有基底が一致した場合には前記乱数信号を信号とし、前記乱数基底と前記共有基底が一致しない場合には前記ダミー乱数を信号とし、これにより各乱数基底の信号が決まり、次の基底決定の過程において前記乱数基底に一致しなかった前記共有基底と次の乱数基底との照合を行い、一致すれば前記乱数信号を信号とし、一致しなければ前記ダミー乱数を信号とし、前記共有基底が前記乱数基底に一致するまで照合と信号決定の処理を繰り返し、前記共有基底と前記乱数基底の一致後は次の共有基底に進んで同様の処理を繰り返し、

前記第1の光源からの出力光に前記第1の変調器により、前記乱数基底で前記信号を重畳して第1の信号光とし、

その際、前記第1の光源からの出力光は揺らぎを伴うか、あるいは前記第1の光源又は前記第1の変調器において揺らぎが重畳され、

前記第1の信号光は前記光伝送路に出力され、

前記プライバシアンプは前記第1の乱数発生器の出力である乱数信号のビット数を減らして秘密鍵を生成し、

前記暗号器は前記秘密鍵を用いて送信信号を暗号化し、

前記光送信機から前記暗号化した送信信号によって変調した第2の信号光を出力し、

前記受信機は、前記第1の光検出器で前記第1の信号光を受信し、

乱数基底及び信号の値を判定し、受信した乱数基底と前記共有基底とを照合し、一致するまで前記共有基底と乱数基底との照合を繰り返し、一致した場合に信号を乱数信号として扱い、次の共有基底に進んで同様の処理を繰り返し、

以上の一連の過程により得られた信号を誤り訂正符号化された乱数信号として前記誤り訂正復号器で復号し、

前記プライバシアンプによってビット数を減らして秘密鍵を取り出し、

前記第2の光検出器で前記第2の信号光を受信し、

前記取り出した秘密鍵を用いて前記暗号復号器で、前記第2の光検出器で受信した信号から前記送信信号を復号することを特徴とする暗号通信システム。

[3] 第1の乱数発生器、誤り訂正符号器、第2の乱数発生器、第3の乱数発生器、第1の擬似乱数発生器、第2の擬似乱数発生器、第1の光源、第1の変調器、プライバシアンプ、暗号器、並びに第2の光源及び第2の変調器を有する光送信機を具備する送信機と、

第1の光検出器、第1の擬似乱数発生器、第2の擬似乱数発生器、誤り訂正復号器、プライバシアンプ、第2の光検出器、及び暗号復号器を具備する受信機と、

前記送信機と前記受信機をつなぐ光伝送路とを有し、

前記送信機と前記受信機は予め乱数からなる第1の種鍵と第2の種鍵を共有し、前記第1の種鍵は前記送信機内及び前記受信機内それぞれの第1の擬似乱数発生器を通して共有基底を与え、前記第2の種鍵は前記送信機内及び前記受信機内それぞれの第2の擬似乱数発生器を通して前記共有基底を利用する信号スロットを与え、

前記送信機は、前記第1の乱数発生器の出力を乱数信号として前記誤り訂正符号器によって誤り訂正符合化し、

前記第2の乱数発生器の出力をダミー乱数とし、前記第3の乱数発生器の出力をダミーの乱数基底とし、

前記共有基底を利用する信号スロットでは前記共有基底を用いて前記乱数信号を信号とし、前記共有基底を利用しない信号スロットでは前記ダミーの乱数基底を用いて前記ダミー乱数を信号とし、

前記第1の光源からの出力光に前記第1の変調器を用いて前記信号を重畳して第1の信号光とし、

その際、前記光源からの出力光は揺らぎを伴うか、あるいは前記光源又は前記変調器において揺らぎが重畳され、

前記第1の信号光は前記光伝送路に出力され、

前記プライバシアンプは前記第1の乱数発生器の出力である乱数信号のビット数を減らして秘密鍵を生成し、

前記暗号器は前記秘密鍵を用いて送信信号を暗号化し、

前記光送信機から前記暗号化した送信信号によって変調した第2の信号光を出力し、

前記受信機は、前記第1の光検出器で前記第1の信号光を受信し、

前記共有基底の信号スロットで伝送されてきた信号を乱数信号として前記誤り訂正復号器で復号し、

前記プライバシアンプによってビット数を減らして秘密鍵を取り出し、

前記第2の光検出器で前記第2の信号光を受信し、

前記取り出した秘密鍵を用いて前記暗号復号器で、前記第2の光検出器で受信した信号から前記送信信号を復号することを特徴とする暗号通信システム。

[4] 請求項1～3のいずれか1項記載の暗号通信システムにおいて、前記第1の光源からの出力光の揺らぎは位相揺らぎあるいは強度揺らぎであること、又は前記第1の光源あるいは前記第1の変調器によって重畳される揺らぎは前記第1の信号光に位相揺らぎあるいは強度揺らぎを与えるものであることを特徴とする暗号通信システム。

[5] 請求項1又は2記載の暗号通信システムにおいて、前記送信機と前記受信機は予め第2の種鍵を共有し、前記送信機では、前記第1の乱数発生器から発生された乱数信号を前記第2の種鍵により暗号化したのち前記誤り訂正符号器によって誤り訂正符号化し、前記受信機では、前記前記誤り訂正復号器で復号された信号を前記第2の種鍵を用いて復号することを特徴とする暗号通信システム。

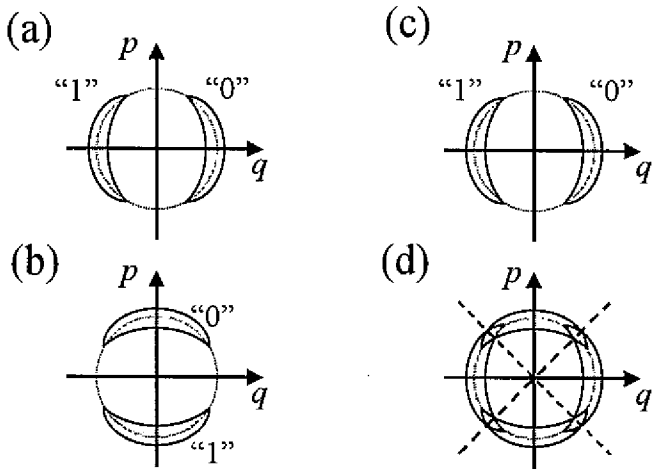
[6] 請求項3記載の暗号通信システムにおいて、前記送信機と前記受信機は予め第3の種鍵を共有し、前記送信機では、前記第1の乱数発生器から発生された乱数信号を前記第3の種鍵により暗号化したのち前記誤り訂正符号器によって誤り訂正符号化し、前記受信機では、前記誤り訂正復号器で復号された信号を前記第3の種鍵を用いて復号することを特徴とする暗号通信システム。

[7] 請求項1～3のいずれか1項記載の暗号通信システムにおいて、前記乱数信号及び前記ダミー乱数は2値とし、前記乱数基底は2基底とし、合わせて4値の状態で信号が伝送されることを特徴とする暗号通信システム。

[8] 請求項1～3のいずれか1項記載の暗号通信システムにおいて、前記乱数信号及び前記ダミー乱数はn値とし、前記乱数基底はm基底とし、合わせてn×m値の状態で信号が伝送されることを特徴とする暗号通信システム。

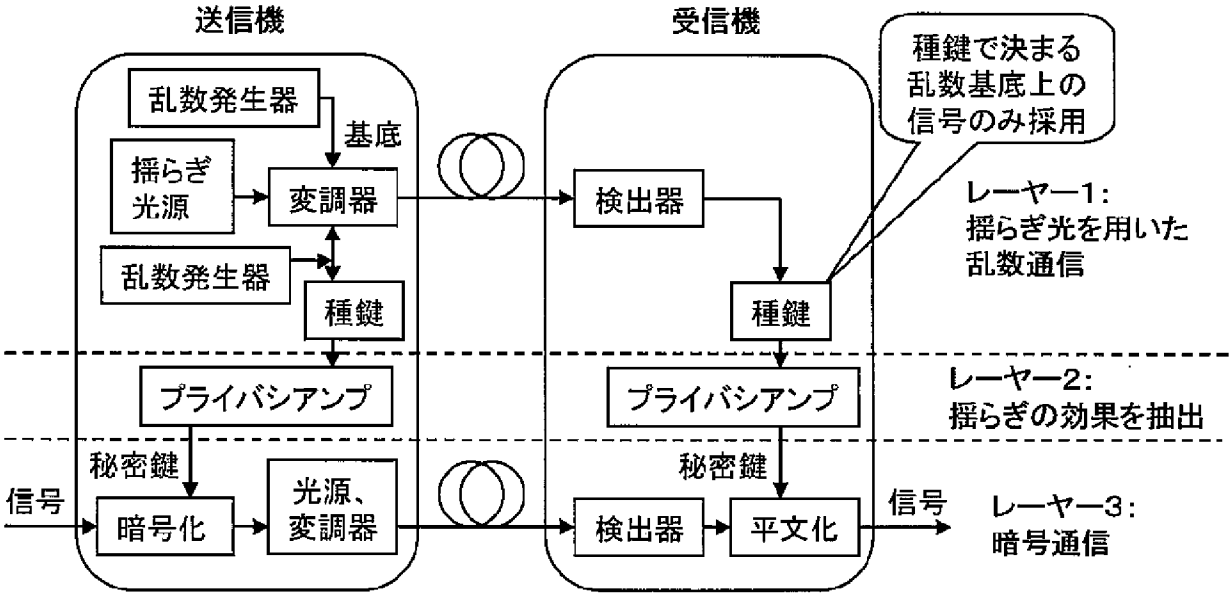
[図1]

図1

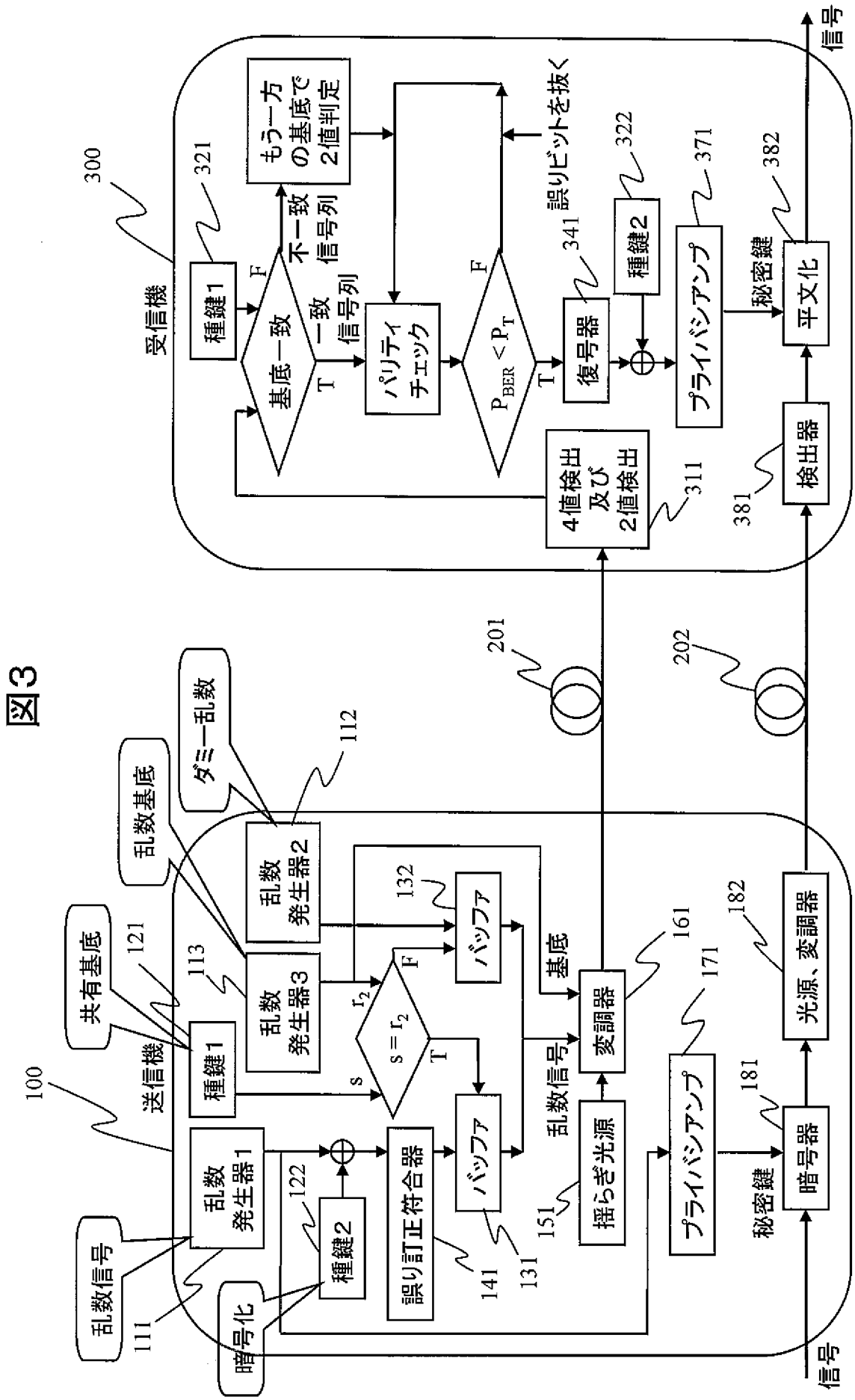

(a)
p
"1"
"0"
q
(c)
p
"1"
"0"
q
(b)
p
"0"
q
"1"
(d)
p
q

[図2]

図2

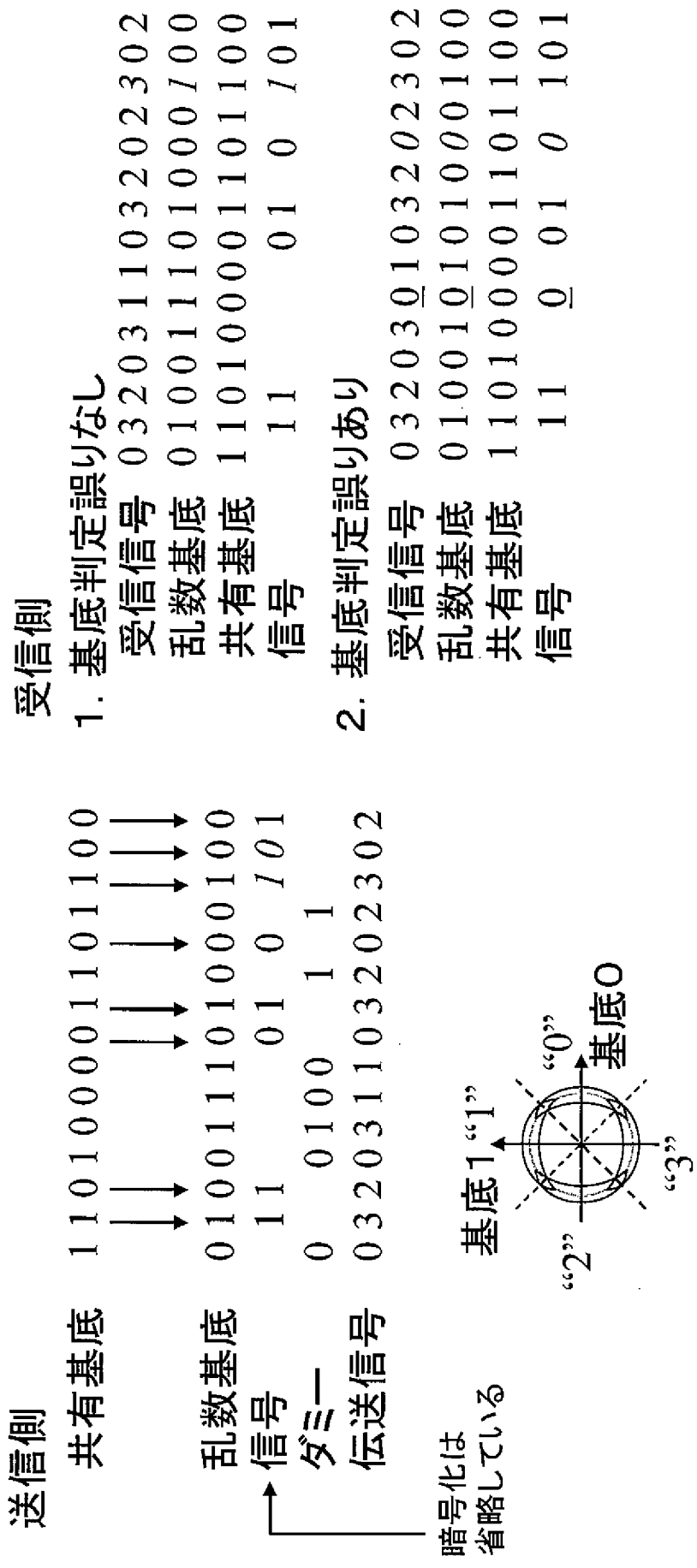

送信機
受信機
乱数発生器
基底
揺らぎ光源
変調器
乱数発生器
種鍵
プライバシアンプ
秘密鍵
信号
暗号化
光源、変調器
検出器
種鍵
プライバシアンプ
秘密鍵
検出器
平文化
信号
種鍵で決まる乱数基底上の信号のみ採用
レーヤー1:揺らぎ光を用いた乱数通信
レーヤー2:揺らぎの効果を抽出
レーヤー3:暗号通信

[図3]


図3
送信機
100
乱数信号
111
乱数発生器1
暗号化
種鍵1
121
共有基底
乱数基底
ダミー乱数
乱数発生器3
113
乱数発生器2
112
種鍵2
122
誤り訂正符合器
141
バッファ
131
バッファ
132
s
$s = r_2$
r_2
F
T
基底
乱数信号
揺らぎ光源
151
変調器
161
プライバシアンプ
171
暗号器
秘密鍵
181
光源、変調器
182
信号
201
202
受信機
300
種鍵1
321
基底一致
F
T
一致信号列
不一致信号列
もう一方の基底で2値判定
パリティチェック
$P_{BER} < P_T$
F
T
誤りビットを抜く
341
復号器
種鍵2
322
プライバシアンプ
371
秘密鍵
平文化
382
4値検出及び2値検出
311
検出器
381
信号

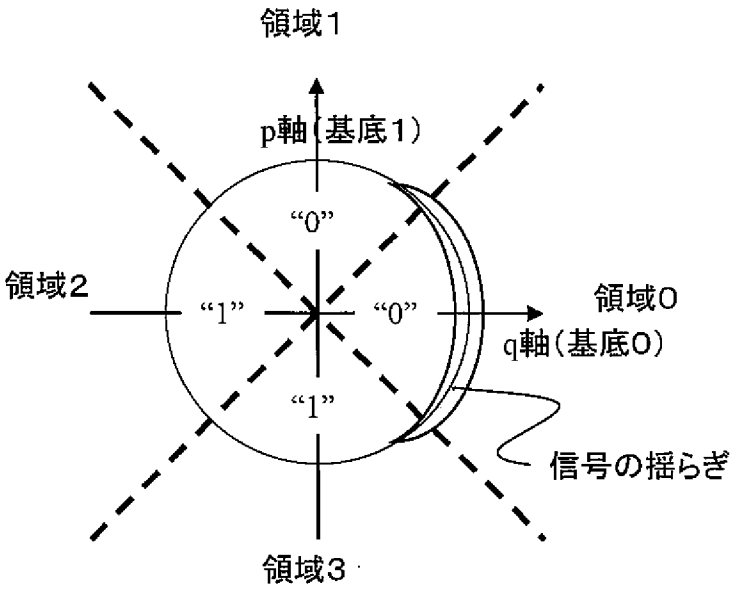
[図4]

図4


送信側
共有基底 1 1 0 1 0 0 0 1 1 0 1 1 0 0
乱数基底 0 1 0 0 1 1 1 0 1 0 0 0 1 0 0
信号 1 1 0 1 0 1 0 1
ダミー 0 0 1 0 0 1 1
伝送信号 0 3 2 0 3 1 1 0 3 2 0 2 3 0 2
暗号化は省略している
受信側
1. 基底判定誤りなし
受信信号 0 3 2 0 3 1 1 1 0 3 2 0 2 3 0 2
乱数基底 0 1 0 0 1 1 1 1 0 1 0 0 0 1 0 0
共有基底 1 1 0 1 0 0 0 0 1 1 0 1 1 0 0
信号 1 1 0 1 0 1 0 1
2. 基底判定誤りあり
受信信号 0 3 2 0 3 0 1 0 3 2 0 2 3 0 2
乱数基底 0 1 0 0 1 0 1 0 1 0 0 0 1 0 0
共有基底 1 1 0 1 0 0 0 0 1 1 0 1 1 0 0
信号 1 1 0 1 0 1 0 1
基底1
“1”
“0”
基底0
“2”
“3”

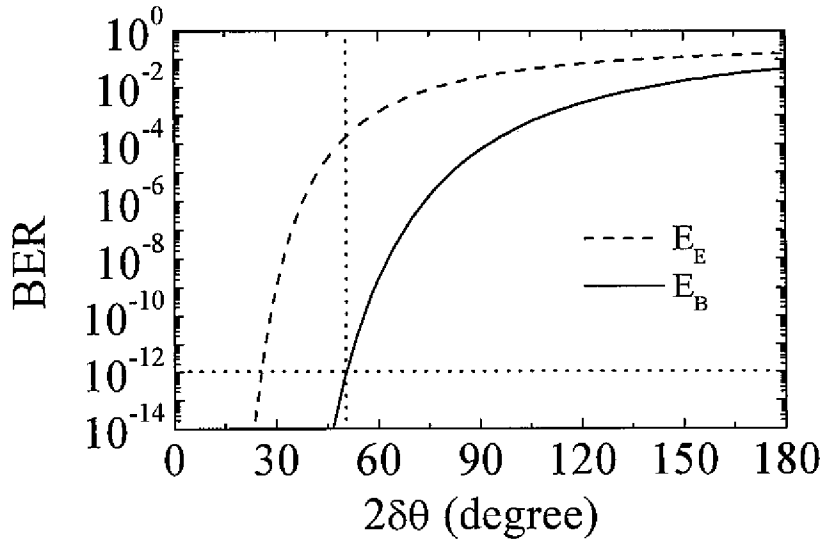
[図5]

図5

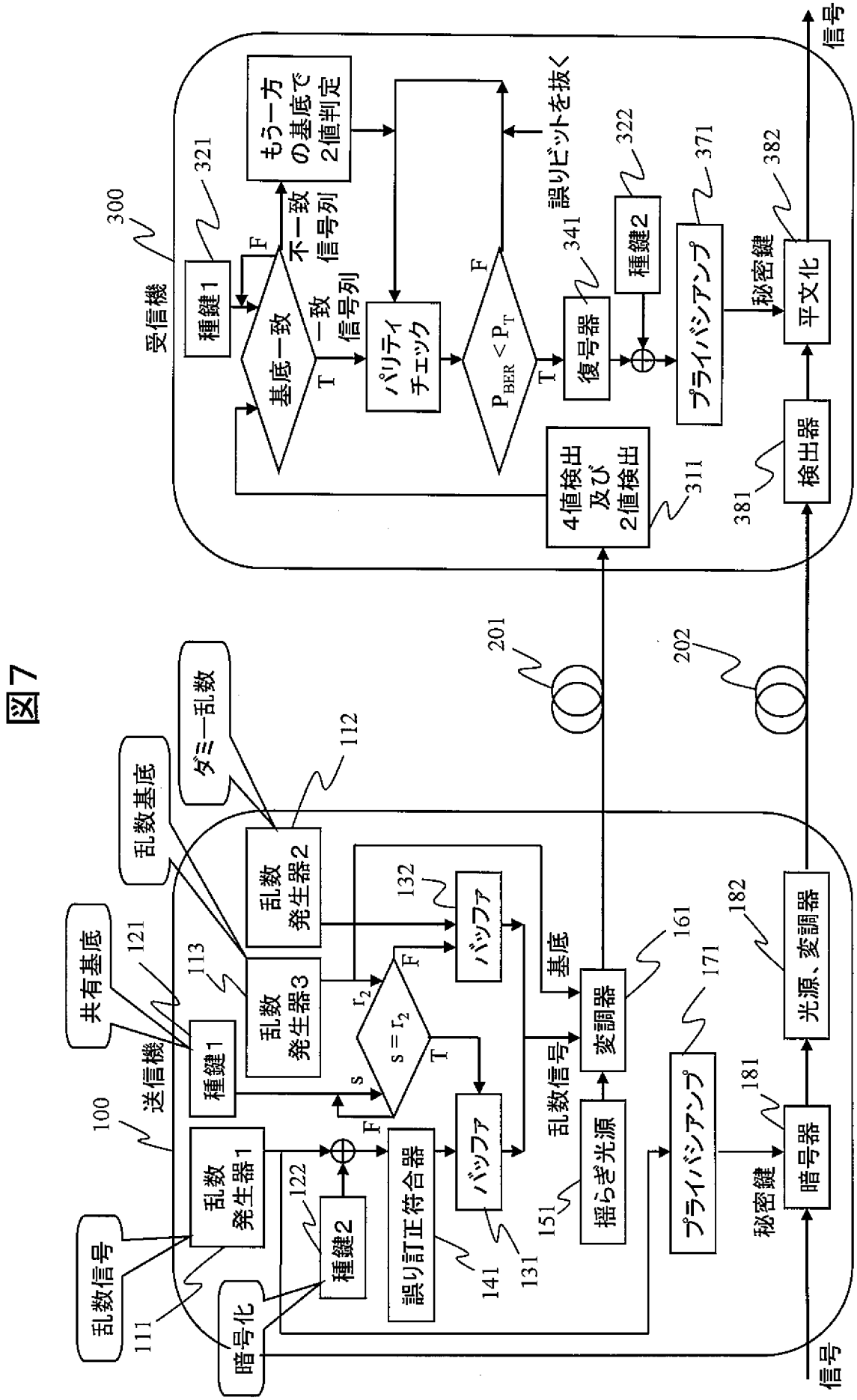

領域1
p軸（基底1）
“0”
領域2
“1”
“0”
領域0
q軸（基底0）
“1”
信号の揺らぎ
領域3

[図6]

図6

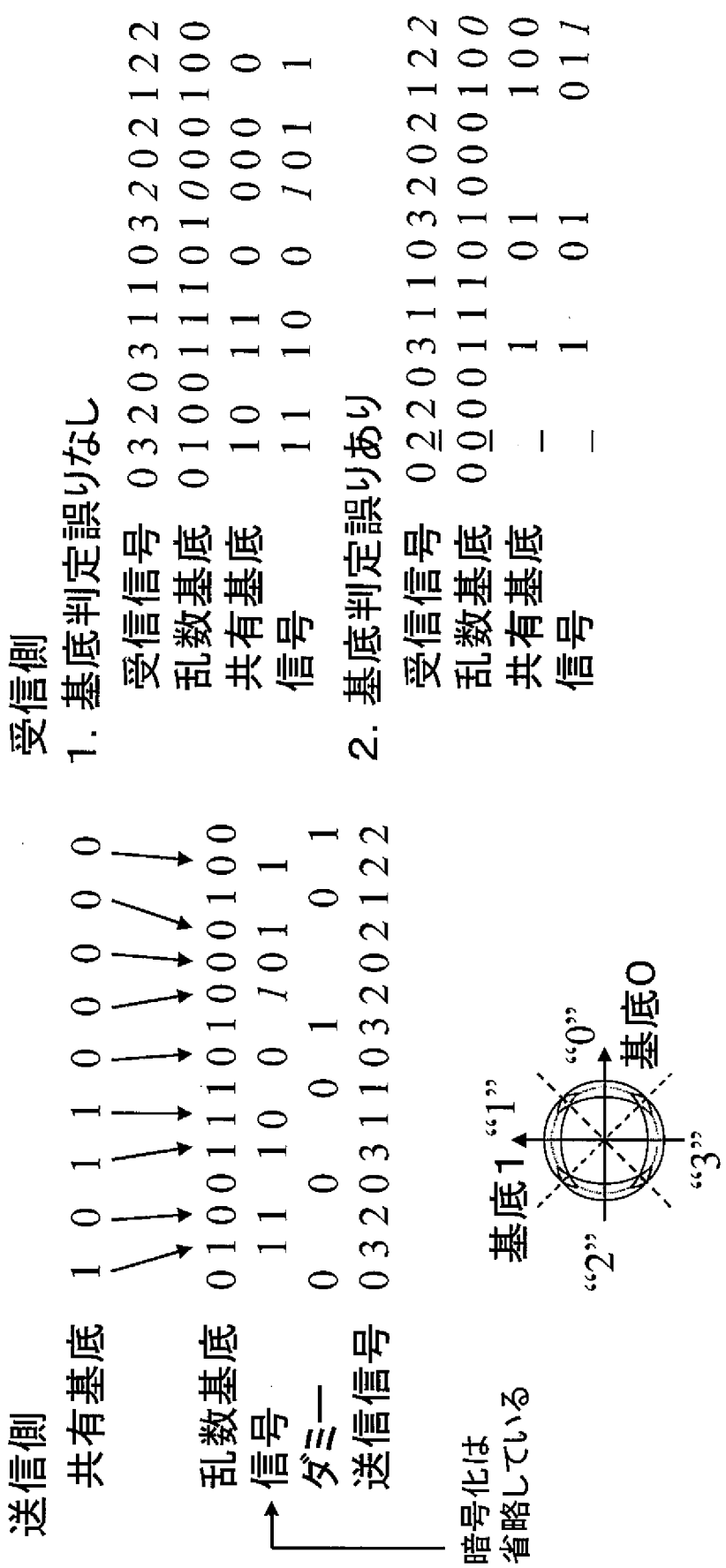

BER
10^{0}
10^{-2}
10^{-4}
10^{-6}
10^{-8}
10^{-10}
10^{-12}
10^{-14}
0 30 60 90 120 150 180
2δθ (degree)
E_E
E_B

[図7]

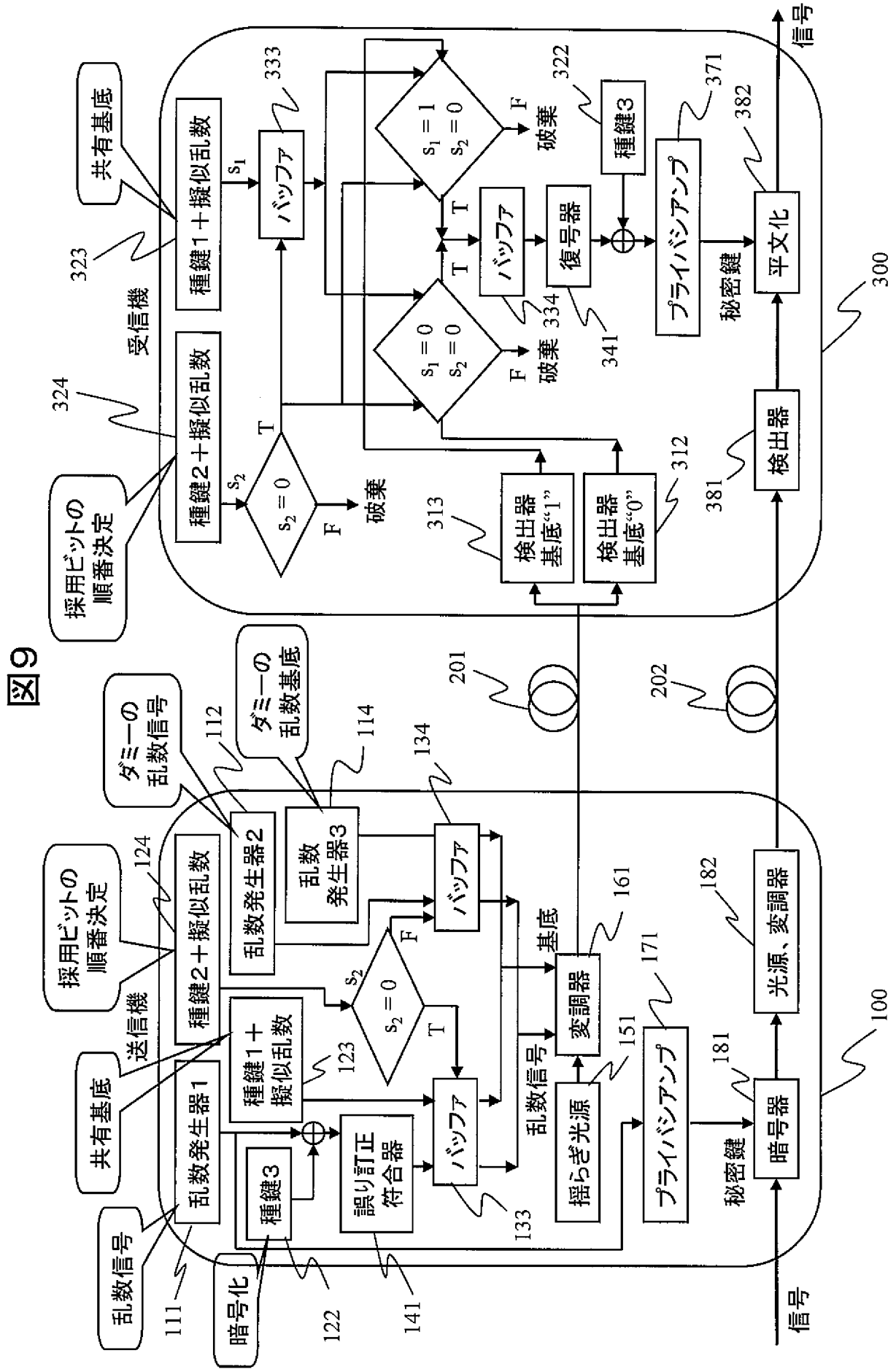

図7
送信機
100
乱数信号
111
乱数発生器1
暗号化
種鍵1
121
共有基底
乱数基底
ダミー乱数
乱数発生器3
乱数発生器2
112
113
種鍵2
122
誤り訂正符合器
141
バッファ
131
バッファ
132
s = r2
s
r2
F
T
乱数信号
基底
揺らぎ光源
151
変調器
161
プライバシアンプ
171
光源、変調器
182
暗号器
181
秘密鍵
信号
201
202
受信機
300
種鍵1
321
基底一致
F
T
一致信号列
不一致信号列
もう一方の基底で2値判定
パリティチェック
P_BER < P_T
誤りビットを抜く
341
復号器
種鍵2
322
プライバシアンプ
371
秘密鍵
382
平文化
4値検出及び2値検出
311
検出器
381
信号

[図8]

図8

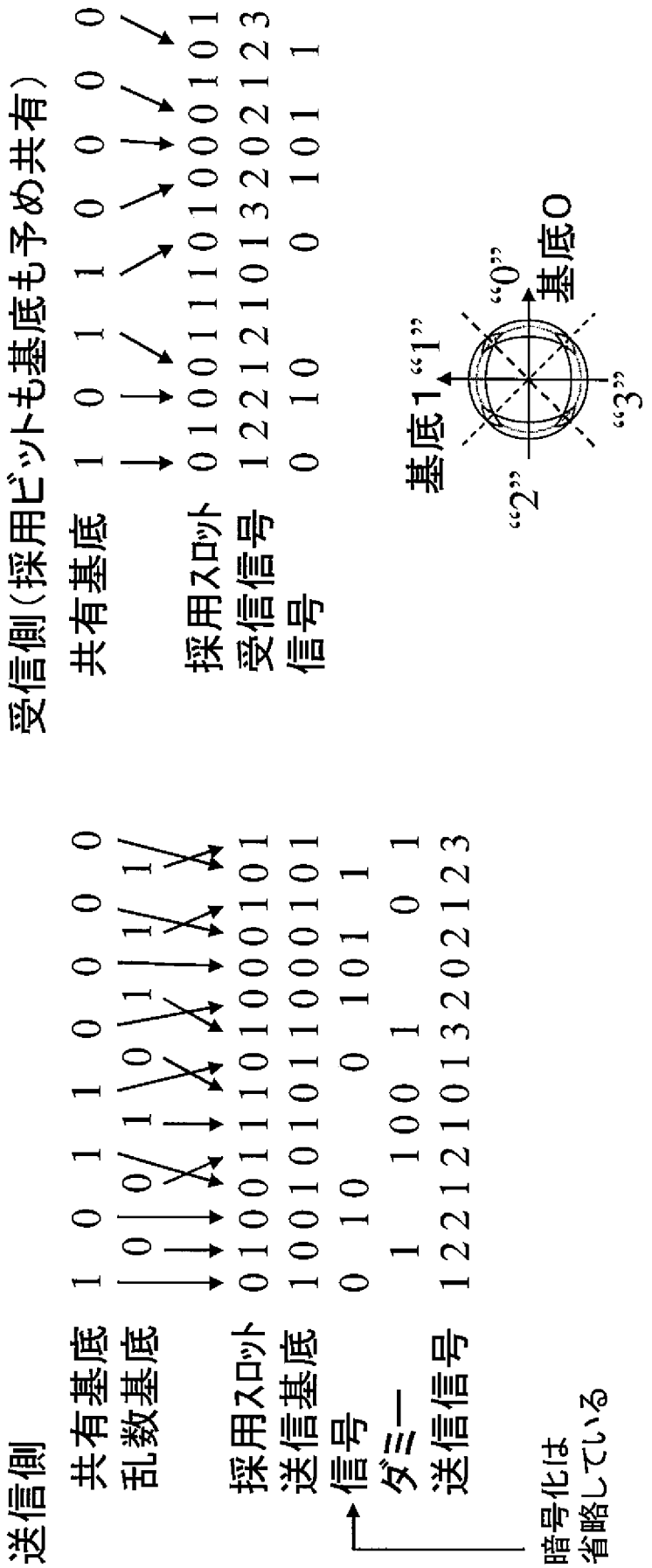

送信側
共有基底 1 0 1 1 0 0 0 0 0 0
乱数基底 0 1 0 0 1 1 1 0 1 0 0 0 1 1 0 0 1 0 0
信号 1 1 1 0 0 1 0 1 1
ダミー 0 0 0 1 0 1
送信信号 0 3 2 0 3 1 1 0 3 2 0 2 1 2 2
暗号化は省略している
受信側
1. 基底判定誤りなし
受信信号 0 3 2 0 3 1 1 1 0 3 2 0 2 1 2 2
乱数基底 0 1 0 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 1 0 0
共有基底 1 0 1 1 0 0 0 0 0 0
信号 1 1 1 0 0 1 0 1 1
2. 基底判定誤りあり
受信信号 0 2 2 0 3 1 1 0 3 2 0 2 1 2 2
乱数基底 0 0 0 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 1 0 0
共有基底 – 1 0 1 1 0 0
信号 – 1 0 1 0 1 1
基底1
“1”
“0”
基底0
“2”
“3”

[図9]


図9
乱数信号
111
暗号化
乱数発生器1
種鍵3
122
種鍵1＋擬似乱数
123
誤り訂正符合器
141
バッファ
133
乱数信号
基底
揺らぎ光源
151
変調器
161
送信機
共有基底
採用ビットの順番決定
124
種鍵2＋擬似乱数
乱数発生器2
112
ダミーの乱数信号
乱数発生器3
114
ダミーの乱数基底
134
バッファ
$s_2 = 0$
T
F
破棄
プライバシアンプ
171
秘密鍵
181
暗号器
光源、変調器
182
100
信号
201
202
受信機
共有基底
323
採用ビットの順番決定
324
種鍵1＋擬似乱数
種鍵2＋擬似乱数
s_1
s_2
バッファ
333
$s_1 = 1$ $s_2 = 0$
$s_1 = 0$ $s_2 = 0$
破棄
322
種鍵3
バッファ
334
復号器
341
プライバシアンプ
371
秘密鍵
382
平文化
検出器
381
検出器基底“1”
313
検出器基底“0”
312
300
信号

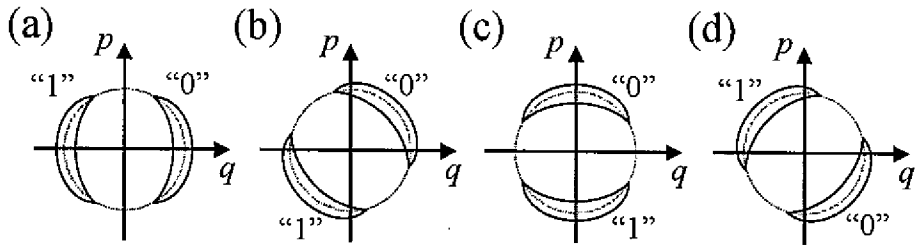
[図10]

図10


送信側
共有基底 1 0 1 1 0 0 0 0
乱数基底 0 0 1 0 1 1 1 1
採用スロット 0 1 0 0 1 1 1 0 1 0 0 0 1 1 0 1
送信基底 1 0 0 1 0 1 1 0 1 1 1 0 0 0 1 0 1
信号 0 1 0 0 1 0 1 1
ダミー 1 1 0 0 1 0 1
送信信号 1 2 2 1 2 1 0 1 3 2 0 2 1 2 3
暗号化は
省略している
受信側(採用ビットも基底も予め共有)
共有基底 1 0 1 1 0 0 0 0
採用スロット 0 1 0 0 1 1 1 0 1 0 0 0 1 1 0 1
受信信号 1 2 2 1 2 1 0 1 3 2 0 2 1 2 3
信号 0 1 0 0 1 0 1 1
基底1 "1"
"0"
基底0
"2"
"3"

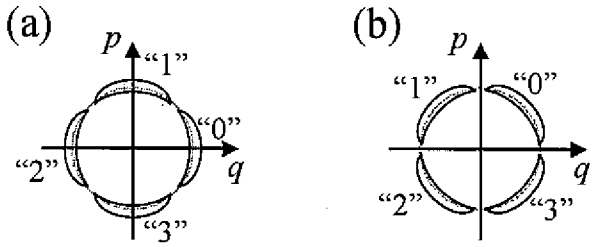
[図11]

図11



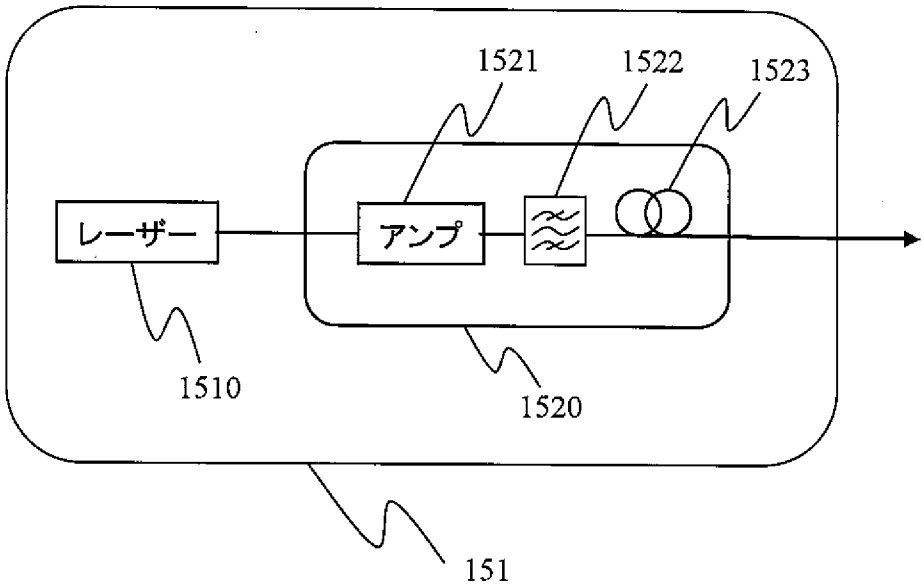
[図12]

図12



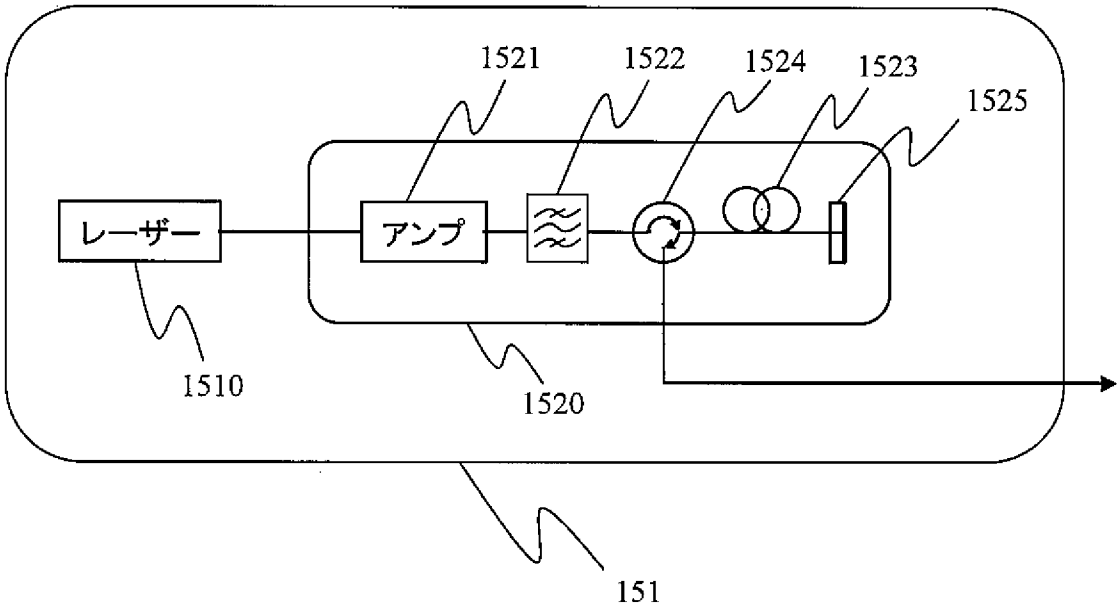
[図13]

図13



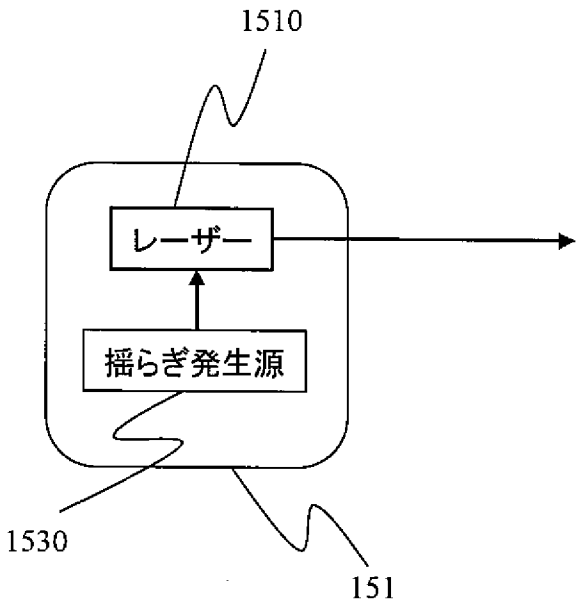
[図14]

図14



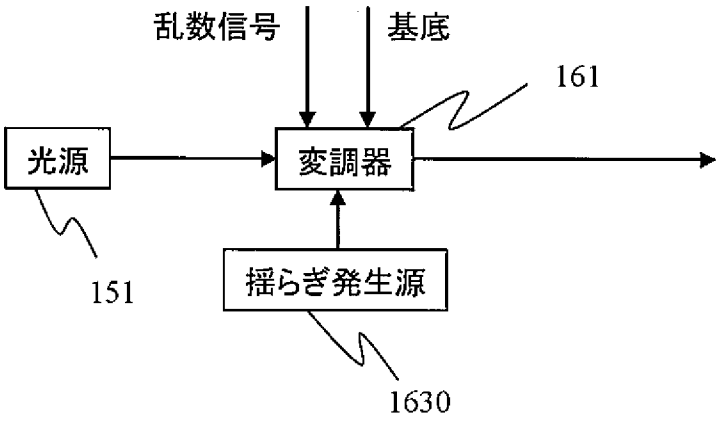
[図15]

図15



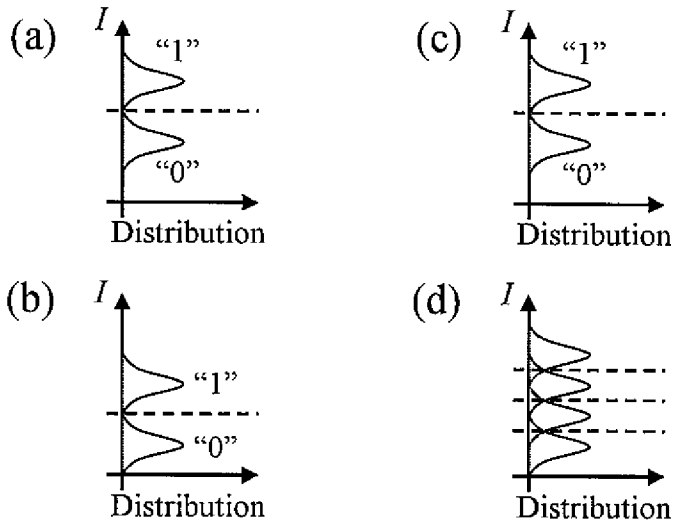
[図16]

図16



[図17]

図17



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/054653

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/12(2006.01)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)
H04L9/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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	Horace P. Yuen et.al., Security of Y-00 and similar quantum cryptographic protocols, [online], arxiv.org, 2004.11.12, .1-9, [retrieved on 2009-04-17] Retrieved from the Internet:<URL:http://arxiv.org/PS_cache/quant-ph/pdf/0407/0407067v2.pdf>	1-8
A	JP 2008-245053 A (Hitachi Information & Communication Engineering, Ltd.), 09 October, 2008 (09.10.08), Par. Nos. [0015] to [0037] (Family: none)	1-8
A	JP 2008-92484 A (Hitachi, Ltd.), 17 April, 2008 (17.04.08), Par. Nos. [0021] to [0046] & US 2008/0085121 A1	1-8

☒ 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
17 April, 2009 (17.04.09)	12 May, 2009 (12.05.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/054653

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7333611 B1 (Northwestern University), 19 February, 2008 (19.02.08), Column 6, line 11 to page 25, line 41 (Family: none)	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０５４６５３

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

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

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	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９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	Horace P. Yuen et.al., Security of Y-00 and similar quantum cryptographic protocols, [online], arxiv.org, 2004.11.12, .1-9, [retrieved on 2009-04-17] Retrieved from the Internet:<URL: http://arxiv.org/PS_cache/quant-ph/pdf/0407/0407067v2.pdf>	1-8
A	JP 2008-245053 A (日立情報通信エンジニアリング株式会社) 2008.10.09, 【0015】～【0037】段落（ファミリーなし）	1-8

☑　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
１７．０４．２００９	１２．０５．２００９

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　３８５７
鳥居　稔
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 2008-92484 A (株式会社日立製作所) 2008.04.17, 【0021】～【0046】段落 & US 2008/0085121 A1	1-8
A	US 7333611 B1 (Northwestern University) 2008.02.19, 第６欄第１１行目～第２５頁第４１行目（ファミリーなし）	1-8