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

特許第5710521号
(P5710521)

(45)発行日　平成27年4月30日(2015.4.30)　(24)登録日　平成27年3月13日(2015.3.13)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
H04L 9/12 (2006.01)　H04L 9/00 631

請求項の数 15　(全 16 頁)

(21)出願番号　特願2012-33014(P2012-33014)
(22)出願日　平成24年2月17日(2012.2.17)
(65)公開番号　特開2013-172182(P2013-172182A)
(43)公開日　平成25年9月2日(2013.9.2)
審査請求日　平成26年6月3日(2014.6.3)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110001689
青稜特許業務法人
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　戸丸　辰也
東京都国分寺市東恋ヶ窪一丁目２８０番地
株式会社日立製作所　中央研究所内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】高セキュリティ通信システム、並びにそれに用いる送信機及び受信機

(57)【特許請求の範囲】
【請求項１】
信号源と、
前記信号源を構成要素とする送信機と該送信機からの信号を受信する受信機との間で共有する共通鍵を用いてパリティ検査記号を決定するパリティ検査記号生成部と、
前記信号源からの出力列のパリティと前記パリティ検査記号とが一致するように調整ビットを該出力列に付加して信号列を生成する調整ビット挿入部とを有することを特徴とする送信機。
【請求項２】
前記信号源は、乱数発生器であることを特徴とする請求項１に記載の送信機。
【請求項３】
前記乱数発生器が出力する乱数列の情報量を縮小する処理を行い、該情報量の縮小された乱数列を秘密鍵として出力する秘密鍵生成部と、
該秘密鍵により実データを暗号化する暗号器とを備え、
該暗号化した実データを送信することを特徴とする請求項２に記載の送信機。
【請求項４】
前記信号列に揺らぎが重畳されていることを特徴とする請求項１に記載の送信機。
【請求項５】
前記信号源を乱数発生器で構成し、
前記受信機との間で予め共有された前記共通鍵を２分割して第１の共通鍵及び第２の共

通鍵とし、
前記乱数発生器を第１の乱数発生器、第２の乱数発生器、第３の乱数発生器に３分割し、
前記第１の共通鍵に基づいて共有基底を決定し、
前記第２の共通鍵を利用してパリティ検査記号生成部でパリティ検査記号を決定し、
前記第１の乱数発生器により信号列１を生成し、
前記第２の乱数発生器により信号列２を生成し、
前記第３の乱数発生器の出力によりランダム基底を決定し、
前記共有基底と前記ランダム基底の比較により、前記信号列の各位置での値が前記信号列１に属するのか前記信号列２に属するのかを決定し、
前記信号列１及び前記信号列２の少なくとも一方の信号列のパリティが前記パリティ検査記号に一致するように調整ビットを該少なくとも一方の信号列に付加し、
前記信号列１及び信号列２の合成信号列を前記ランダム基底により送信することを特徴とする請求項１に記載の送信機。
【請求項６】
前記信号列１及び信号列２の少なくとも一方の情報量を縮小する処理を行い、該縮小された信号列を秘密鍵として出力する秘密鍵生成部と、
該秘密鍵により実データを暗号化する暗号器とを備え、
該暗号化した実データを送信することを特徴とする請求項５に記載の送信機。
【請求項７】
送信機から伝送された信号列を検出する信号検出部と、
前記信号検出部で検出された信号のパリティを算出するパリティ算出部と、
前記信号列を受信する受信機と前記送信機との間で共有する共通鍵を用いてパリティ検査記号を決定するパリティ検査記号生成部と、
前記パリティ検査記号を利用して前記パリティ算出部で算出されたパリティを検査するパリティ検査部とを有することを特徴とする受信機。
【請求項８】
前記送信機との間で予め共有された前記共通鍵を２分割して第１の共通鍵及び第２の共通鍵とし、
前記第１の共通鍵に基づいて共有基底を決定し、
前記第２の共通鍵を利用して前記パリティ検査記号生成部でパリティ検査記号を決定し、
前記信号検出部で得られた前記信号列の受信結果からランダム基底を判定し、
前記ランダム基底と前記共有基底の比較により信号列１と信号列２の分類を行ない、
前記信号列１と前記信号列２の少なくとも一方のパリティをパリティ検査部で前記パリティ検査記号と照合し、
前記パリティにパリティ誤りがあった場合は前記ランダム基底の判定を訂正し、
再度、前記パリティの照合を行ない、前記ランダム基底の訂正と前記パリティの照合を正しいパリティが得られるまで繰り返すことにより、
正しいランダム基底と正しい信号列１、信号列２を得ることを特徴とする請求項７に記載の受信機。
【請求項９】
前記信号列１及び信号列２の少なくとも一方の情報量を縮小する処理を行い、該縮小された信号列を秘密鍵として出力する秘密鍵生成部と、
送信機から暗号化して送られてきた実データを該秘密鍵により復号する復号部とを有することを特徴とする請求項８に記載の受信機。
【請求項１０】
送信機と受信機と前記送信機からの信号を前記受信機に伝送する伝送路とを備え、
該送信機と該受信機は共通鍵を共有し、
前記送信機は、

信号源と、前記共通鍵を用いてパリティ検査記号を決定するパリティ検査記号生成部と、前記信号源からの出力列のパリティと前記パリティ検査記号とが一致するように調整ビットを該出力列に付加して信号列を生成する調整ビット挿入部とを有し、
前記受信機は、
前記送信機から伝送された信号を検出する信号検出部と、
前記信号検出部で検出された信号のパリティを算出するパリティ算出部と、
前記共通鍵を用いてパリティ検査記号を決定するパリティ検査記号生成部と、
前記パリティ検査記号を利用して前記算出されたパリティを検査するパリティ検査部とを有することを特徴とする通信システム。
【請求項１１】
前記信号源を乱数発生器で構成し、
前記送信機と前記受信機との間で予め共有された前記共通鍵を２分割して第１の共通鍵及び第２の共通鍵とし、
前記送信機において、
該乱数発生器を第１の乱数発生器、第２の乱数発生器、第３の乱数発生器に３分割し、
前記第１の共通鍵に基づいて共有基底を決定し、
前記第２の共通鍵を利用してパリティ検査記号生成部でパリティ検査記号を決定し、
前記第１の乱数発生器により信号列１を生成し、
前記第２の乱数発生器により信号列２を生成し、
前記第３の乱数発生器の出力によりランダム基底を決定し、
前記共有基底と前記ランダム基底の比較により、前記信号列の各位置での値が前記信号列１に属するのか前記信号列２に属するのかを決定し、
前記信号列１及び前記信号列２の少なくとも一方の信号列のパリティが前記パリティ検査記号に一致するように調整ビットを該少なくとも一方の信号列に付加し、
前記信号列１及び信号列２の合成信号列を前記ランダム基底を用いて送信し、
前記受信機において、
前記第１の共通鍵に基づいて共有基底を決定し、
前記第２の共通鍵を利用してパリティ検査記号生成部でパリティ検査記号を決定し、
前記信号検出部で得られた前記信号列の受信結果からランダム基底を判定し、
前記ランダム基底と前記共有基底の比較により信号列１と信号列２の分類を行ない、
前記信号列１と前記信号列２の少なくとも一方のパリティをパリティ検査部で前記パリティ検査記号と照合し、
前記パリティにパリティ誤りがあった場合は、前記ランダム基底の判定を訂正し、
再度、前記パリティの照合が行ない、前記ランダム基底の訂正と前記パリティの照合を正しいパリティが得られるまで繰り返すことにより、
正しいランダム基底と正しい信号列１、信号列２を得ることを特徴とする請求項１０に記載の通信システム。
【請求項１２】
前記送信機及び前記受信機において、
前記信号列１及び信号列２の少なくとも一方の情報量を縮小する処理を行い、該縮小された信号列を秘密鍵とし、
前記送信機においては、該秘密鍵により実データを暗号化して送信し、
前記受信機においては、送信機から暗号化して送られてきた実データを該秘密鍵により復号することを特徴とする請求項１１に記載の通信システム。
【請求項１３】
前記信号源は、乱数発生器であることを特徴とする請求項１０に記載の通信システム。
【請求項１４】
前記乱数発生器が出力する乱数列の情報量を縮小する処理を行い、該情報量の縮小された乱数列を秘密鍵として出力する秘密鍵生成部と、
該秘密鍵により実データを暗号化する暗号器とを備え、

該暗号化した信号を送信することを特徴とする請求項１３に記載の通信システム。
【請求項１５】
前記送信機からの出力信号列に揺らぎが重畳されていることを特徴とする請求項１０に記載の通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、高セキュリティ通信システム、並びにそれに用いる送信機及び受信機に係り、特に光通信において安全性を向上させた通信システム、並びにそれに用いる送信機及び受信機に関する。
【背景技術】
【０００２】
ネットワークにより世界中が結ばれた現在、通信における安全性（秘匿性）は通信システムに要求される重要仕様のひとつである。この重要性に基づき、量子暗号の研究が活発に進められてきた（例えば、非特許文献１を参照）。量子暗号は物理法則的に安全性を保証するもので安全性の観点からは最強のものと考えられているが、微視的世界を支配する量子力学にその理論的根拠を置いているために、現実的環境下で運用するには制限事項が多く、通常の光通信システムに導入することは難しい。
【０００３】
そこで、その問題点を解消するものとして、安全性と利便性のバランスした「位相揺らぎを利用した安全な光通信法」が考案された（例えば、非特許文献２を参照）。この方式は位相揺らぎの大きいキャリア光を利用するのが特徴で、大きい位相揺らぎのために不正受信者による盗聴があったとしても十分には情報が漏れない。正規受信者は送信者との間で予め共通鍵を共有しているものとし、これにより正規受信者はノイズの多い信号の中から正しい信号を抜き出すことができる。
【０００４】
正規受信者は共通鍵を利用して不正受信者よりも有利な状況を形成できるが、大きい揺らぎが導入されていることもあり正規受信者においても受信信号にビット誤りがある。そのため、信号に加えてパリティ検査記号を送受信し、受信機において誤り訂正を行う。パリティ検査記号は信号列の並びに付け加えて伝送することも可能であるし、信号列とは別に通常の伝送路を利用して伝送することも可能である（例えば、特許文献１を参照）。
【０００５】
「位相揺らぎを利用した安全な光通信法」は共通鍵と揺らぎの相乗効果を利用する。但し、前述のように揺らぎを利用しているために誤り訂正が必須の重要技術であり、従ってパリティ検査記号の利用法、言い換えれば符号化復号化は本通信法において重要技術との位置付けになる。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】ＷＯ２０１０／１０３６７７号公報
【非特許文献】
【０００７】
【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】T. Tomaru, Jpn. J. Appl. Phys. 74, 074401 (2010)
【発明の概要】
【発明が解決しようとする課題】
【０００８】
上述のように位相揺らぎを利用した安全な光通信法ではビット誤り訂正のためにパリティ検査記号を送受信する。信号列の送受信では大きい揺らぎを伴うキャリア光を利用する

ために、パリティ検査記号を信号列の並びに付け加えて送受信する場合にはパリティ検査記号にもビット誤りが生じる可能性が高くなる。この場合、受信機における誤り訂正の処理が複雑になる。

【０００９】

一方、パリティ検査記号を信号列とは切り離して通常の伝送路で送受信する場合には誤りなく確実に送受信できるが、不正受信者にも確実にパリティ検査記号の情報が知られる可能性があり、通信の安全性を向上させる観点からは好ましくない。理想的には、パリティ検査記号が正確に送受信され、また不正受信者に正確な情報が漏れないことが望まれる。

【００１０】

そこで、本発明の目的は、信号処理の容易さと通信の安全性を両立することが可能な光通信法を提供することである。

【課題を解決するための手段】

【００１１】

本発明の送信機、受信機およびそれらを用いた通信システムにおける技術的特徴は以下の通りである。

【００１２】

送受信者間で共有される共通鍵を利用して信号値とは独立にパリティ検査記号を決定し、パリティ検査記号の情報が不正受信者に漏れることを防止する。その際、信号値に無関係にパリティ検査記号を決定するため、信号列のパリティに整合するように調整用のビットを信号列に加え、信号列のパリティとパリティ検査記号が一致するようにする。

【発明の効果】

【００１３】

パリティ検査記号が共通鍵を利用して決定されるため、パリティ検査記号を安全で且つ確実に送受信者間で共有できる。これにより、信号処理の容易さと通信の安全性を両立することが可能になる。

【図面の簡単な説明】

【００１４】

【図１】本発明による高セキュリティ通信システムの概略を示したブロック図。
【図２】高セキュリティ通信を行うためのプロトコルの概略を示したブロック図。
【図３】直交座標（位相空間）上に示した信号状態を示す図。
【図４】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。
【図５】本発明による高セキュリティ通信システムを実現するための構成例を示す図。
【図６】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。
【図７】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。
【図８】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。
【図９】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。
【図１０】本発明による高セキュリティ通信システムに基づく信号処理の一例を示す図。

【発明を実施するための形態】

【００１５】

以下に、図面を用いて実施例を詳述する。

【実施例１】

【００１６】

本発明の基本形態を図１に示す。送信機100から伝送路200を介して受信機300へ信号源110で発生された信号が伝送される。一般に伝送路中においてビット誤りが生じるため、誤り訂正用の付加ビットが必要である。この付加ビットをパリティ検査記号と呼ぶ。本発明では、送信機100内の共通鍵120と受信機300内の共通鍵320を予め送受信者間での共通鍵として共有し、その共通鍵を利用してパリティ検査記号を生成する。その際、パリティ検査記号に共通鍵をそのまま利用することが可能である。またその共通鍵を元に疑似乱数を発生させ、それをパリティ検査記号とすることも可能である。

【００１７】
パリティ検査記号は、送信機100内では共通鍵120を利用してパリティ検査記号生成部125で生成する。受信機300内では共通鍵120と同一である共通鍵320を利用してパリティ検査記号生成部325においてパリティ検査記号を生成する。パリティ検査記号は信号のビット誤りを訂正するための付加ビットなので、パリティ検査記号は本来信号を元に生成されるべきものであるが、本発明ではパリティ検査記号を信号源110で発生された信号とは独立に決定する。
【００１８】
そのために、信号とパリティ検査記号とを関係づける調整ビットを信号列に追加する。図１の挿入図にその初歩的な一例を符号例１として示す。ここでは５ビットの信号に対して１ビットの調整ビットを加えた場合を示す。図中では信号源110からの信号列の最初の５ビットが“11010”の場合を示す。本符号列１の信号の下段には、共通鍵120を利用して生成されたパリティ検査記号の値を示す。この例では“０”である。
【００１９】
なお、対象とする信号列のパリティはその信号列に現れる“１”の個数で決まる。“１”の個数が偶数ならばパリティ“０”であり、奇数ならばパリティ“１”である。
【００２０】
図中の例では、信号列の最初の５ビットは“１”が３個で奇数となるのでパリティは“１”になる。しかし、共通鍵で決まるパリティ検査記号の最初の値は“０”なので、両者のパリティが一致しない。
【００２１】
そこで、信号列の６ビット目に調整用のビット“１”を加えることにする。この６ビット目を含めて一群の信号列とすれば“１”の個数が偶数となってパリティは“０”となり、共通鍵を元に決めたパリティ検査記号に一致する。最初の信号“11010”の次の信号“01010”に対しても同様な操作を繰り返す。さらに同様な操作を信号列５ビットごとに実施する。
【００２２】
以上の処理の後、信号を送信機から伝送路200を通して受信機300に伝送する。伝送手段としては電気信号や光信号等、いずれの手段でもよい。また、有線でも無線でもよい。
【００２３】
受信機300では検出器310により受信し、その後、パリティ算出部において６ビットごとにパリティを計算する。受信機300内には送信機100内と同じ共通鍵320が予め用意されており、この共通鍵を元に送信機100内と同じ処理を通してパリティ検査記号がパリティ検査記号生成部325で生成される。このパリティ検査記号は先ほど計算したパリティと比較され、伝送中にビット誤りがあったかどうかが判定される。両パリティが一致しない場合は、対象の６ビット中のいずれかがビット誤りを起こしていることになる。
【００２４】
以上のパリティ検査記号の利用法（符号化法）ではビット誤りが生じたところまでは検出できるが訂正まではできない。誤り訂正を可能にするためにはパリティ検査記号をさらに増やす必要がある。その一例を図１の別の挿入図に符号例２として示す。
【００２５】
信号列を行列に並べ、各行各列に対してパリティ検査記号を割り付けて調整用のビットを加える。これは水平垂直符号と呼ばれる符号化を変形したものである。このように符号化しておけば、各行列内の一か所にビット誤りがあった場合に、行パリティと列パリティのそれぞれひとつにビット誤りが生じることになり、誤りビットが特定できて訂正可能になる。この誤り訂正を通して受信機おいて信号が再生される。
【００２６】
以上のパリティ検査符号の利用法（符号化法）は比較的初歩的な利用法であり、各種符号化法を同様に変形すれば本発明に適用可能である。
【実施例２】

【００２７】
実施例１では本発明に関する最も初歩的な利用形態について述べた。しかし、パリティ検査記号に関する本発明は様々な利用形態があり、特に「揺らぎを利用した安全な通信法」において本発明の効果が発揮される。そこで、以下では主として光通信を具体例に挙げて実施例を述べる。また、揺らぎとしてキャリア光の位相揺らぎを取り上げることにする。もちろん、本発明は強度揺らぎに対しても適用可能であると共に、光通信に限らず電気信号を利用した一般の通信、さらに有線に限らず無線通信にも適用可能である。
【００２８】
位相揺らぎを利用した安全な光通信のプロトコルは、３段階のステップからなり、図２に示すように、第１段階での乱数の送受信（鍵配送）、第２段階での送受信された乱数列からの秘密鍵生成、第３段階での生成した秘密鍵を利用した実データの暗号通信からなる（非特許文献２：T. Tomaru, Jpn. J. Appl. Phys. 74, 074401 (2010)を参照）。第２段階の「送受信された乱数列からの秘密鍵生成」は送受信機内の論理演算であり、送受信された乱数列のビット数を減らし、それにより秘密鍵の安全性を増強する（秘匿性の増強）（C. H. Bennett, G. Brassard, C. Crepeau, and U. U. Maurer, “Generalized privacy amplification, ”IEEE Trans. Inf. Theory 41, 1915 (1995)を参照）。本プロトコルでは第１段階と第２段階の処理を通して秘密鍵を生成し、それにより安全性を保証するため、第３段階の「生成した秘密鍵を利用した実データの暗号通信」に関しては通常の暗号通信と同様な形態をとる。
【００２９】
ここで通常の暗号通信とは、伝送路における揺らぎを極力排除した状況で実データを秘密鍵により暗号化して送受信することを意味する。第３段階の「生成した秘密鍵を利用した実データの暗号通信」は通常の暗号通信で安全性の確保は十分であるが、さらに安全性を確保するために、第１段階でのように揺らぎを伴う光を利用することも可能である。
【００３０】
次に第１段階の鍵配送を、揺らぎの効果を含めて説明する。図３（ａ）は位相０と位相πの信号状態を直交座標上に模式的に示したものである（この直交座標系を位相空間と呼ぶ）。(0, π)の信号値は、本来a_1軸上にあるはずのものであるが、「位相揺らぎを利用した安全な光通信法」では信号値に位相揺らぎδθがあるために信号値が正確に(0, π)にならず(0＋δθ, π＋δθ)となる。その結果、(0, π)の信号範囲は、図１（ａ）に示すような三日月状の領域になる（なお、δθは正負の値を取り得る）。図３（ｂ）は、信号値として(π/2, 3π/2)の位相を利用した場合である。
【００３１】
第１段階の鍵配送では“０”及び“１”の乱数を位相0及びπ、あるいは位相π/2及び3π/2として伝送する。どちらの位相の組み合せを利用するかはランダムに決定する。(0, π)の位相を利用する場合を基底0（図３(a)）、(π/2, 3π/2)の位相を利用する場合を基底１と定義する（図３(b)）。信号乱数は(0, 1)の２値であり、またランダムな基底も(0, 1)の２値なので合わせて見かけ上４値になる（図３(c)）。
図３（ｃ）では三日月状の領域（揺らぎの範囲）が重なっておりこれがビット誤りの原因である。
【００３２】
「位相揺らぎを利用した安全な光通信法」では安全な情報量の確保にこのビット誤りを利用する。一般に安全な情報量を確保するためには正規受信者を不正受信者に対して有利な状況にする必要がある。ここでは正規受信者が不正受信者に比べて低いビット誤り率で信号を受信できる状況にする。そのために送信者と正規受信者とで予め共有した共通鍵を利用する。正規受信者はこの共通鍵を利用して位相揺らぎの影響を低減し、低いビット誤り率で受信する。以下はそれを実現するための処理である。
【００３３】
共通鍵は主に２つの目的に利用する。一つは「共有基底」と呼ぶ基底を決定するためであり、もう一方は本発明の主題であるパリティ検査記号を決定するためである。

【００３４】
先ず、共有基底に関して述べる。上述のように鍵配送ではランダムな基底（以下に、「ランダム基底」と呼ぶ）を利用して乱数を送受信する。ここで、不正受信者へ意味のある情報流出を防ぐ狙いで、送受信する乱数をすべて秘密鍵生成のために使うのではなく、半数をダミーとして受信後に破棄することにする。これにより不正受信者はどこに意味のある情報があるのかが分からない。鍵配送で送受信する乱数は、実際に秘密鍵生成に利用する乱数もダミーも共に乱数である。そこで秘密鍵生成に利用する乱数をダミーと区別して「信号乱数」と呼ぶことにする。送受信する乱数のどれが信号乱数でどれがダミーであるかは共通鍵で決まる共有基底とランダム基底との照合により決定することにする。
【００３５】
図４に、その様子を例示する。図４で示す送信機の左欄には、共有基底（共通鍵）、ランダム基底、信号乱数、ダミー、伝送信号、およびパリティ検査記号が示され、それぞれに対応するビット列が右欄に記載されている。各ビット列は、左から右へ順番に第一ビット、第二ビット、・・・と呼ぶことにする。図４に示す受信機も送信機と同様な記述に従うが、基底の判定に誤りがない場合（右上段）と、誤りがある場合（右下段）とに分けて表記している。
【００３６】
図４について具体的に見てみると、送信機側において共有基底の第一ビットは“１”であり、ランダム基底の第一ビットは“０”である。両ビットが不一致なのでダミーの乱数を送るものとする。第二ビットは共有基底とランダム基底の両者が“１”であり、信号乱数を送るものとする。以下同様な取り決めで信号乱数かダミーであるかを決定する。伝送信号は基底分の１ビットと乱数分の１ビットの２ビットで決まるため、図４では４値表現してある。４値の割り振りは図４の挿入図に示す。
【００３７】
受信機では送信機と逆の処理を行う。まず、４値の伝送信号を受信する。図４右側の「受信信号」の項目がそれに相当する。４値の受信信号には基底の情報を含んでおりまず基底の判定を行う。受信信号が“０”及び“２”ならば基底0、“１”及び“３”ならば基底1と判定する。この判定された基底が「ランダム基底」に相当する。受信機は共通鍵を保持しておりこれにより「共有基底」が決まる。送信機の場合と同様にランダム基底と共有基底を比較し、各ビット上の乱数が信号乱数かダミーかを判定する。なお、図４中の受信機側では、乱数の判定結果として信号乱数のみ示しダミーは特に示していない。以上の処理において、受信機において誤りなく受信できた場合は、以上で信号乱数を送受信機間で共有できたことになる。
【００３８】
しかし、実際には受信信号に誤りが発生する場合がある。特に「位相揺らぎを利用した安全な光通信法」ではこの誤りが多くなるような設定をする。受信信号に誤りがある場合の例を図４の右下段に示す。下線部のビットが誤りである。本来、４値判定で“１”であるべきところが“０”になっている。その結果、ダミーであるべきデータが信号乱数として判定される。ダミーと信号乱数の判定誤りを訂正するためにはパリティ検査記号を利用する。
【００３９】
パリティ検査記号は、送受信機間で共有された共通鍵により決定する。しかし、パリティはデータに基づき決まるものなので、データから決まるパリティと共通鍵から決まるパリティは一般に一致しない。そこで両パリティが一致するように信号乱数列に調整用のビットを挿入する。初歩的な例として信号乱数５ビットをひとまとめにし、６ビット目に調整用のビットを加えた例が図４である。
【００４０】
図４の送信機側では、信号乱数の最初の５ビットは“１”が３個、“０”が２個からなり、パリティは“１”になる。しかし共通鍵により決定するパリティ検査記号は“０”である。両パリティが一致しないことになるので調整用のビット“１”を信号乱数列の６ビット

目（斜字体のビット）に挿入する。以下、同様の規則で５ビットの乱数に１ビットの調整ビットを加え、６ビットを一単位とする信号乱数列を形成する。

【００４１】

受信機においては誤りなく受信できれば信号乱数列が再現される。図４の右上段の信号処理例では、送信機側の信号乱数列が再現されている。しかし、判定誤りがあった場合には図４の右下段に示すように信号乱数列とダミー乱数列の判定が誤ることになる。図４の右下段の例では信号乱数列が１ビット余分になる。信号乱数列を６ビットごとに処理する規則に従えば、本来乱数の第５ビットであるはずのビットが調整ビットになってしまう。その結果、図４の右下段の例では、信号乱数列のパリティ（“１”が３個なので“１”）とパリティ検査記号“０”が一致しなくなる。調整ビット位置のずれは後続の全ビットにも起こるので、判定誤りのあった位置以降パリティ不一致は確率１／２で起こる。従って、どの位置に判定誤りがあったかは概ね判る。

【００４２】

そこで、判定誤りがあったと思われるビット位置付近の受信信号の一つに対して判定値を訂正し、ランダム基底と共有基底の判定からすべてやり直してパリティを調べる。この処理を疑わしいビット位置付近のすべてのビットに対して順番に実行すれば全パリティがほぼ一致する訂正が見つかる。このようにして基底の判定誤りが訂正される。

【００４３】

この基底の訂正を通して鍵配送時の基底が受信機において確定することになる。即ち、共通鍵を共有している正規の受信者はこの時点で信号乱数“０”あるいは“１”の２値のみを判定すれば良いことになる。不正受信者は共通鍵を持たないために信号乱数列とダミーを識別することができず、信号の解析では４値信号の判定結果をそのまま使わなければならない。最終的に２値信号として処理できる正規受信者に対して不正受信者は４値信号のまま処理しなければならない。この差が本方法における安全性の起源である。

【００４４】

以上の処理では信号乱数５ビットごとに１ビットの調整ビットを加える方法でパリティ検査記号の利用法を説明した。但し、これは原理を示すための初歩的な利用法であり、実際にはより高度なパリティ検査記号の利用法が適用可能である。例えば、実施例１に示したように信号乱数列を行列に並べ、水平方向と垂直方向の両方向に対してパリティを検査するのもひとつの方法である。また、ここまでは基底の訂正に話を限定したが、基底の訂正が完了しても信号乱数に対するビット誤りが残る。そのため、信号乱数用に別の誤り訂正符号を併用することも有用である。このようにしておけば、基底訂正が不十分で僅かに基底の判定誤りが残ったとしてもビット誤りとして処理することが可能になる。

【００４５】

以上の原理に基づいた送受信機の構成図を図５に示す。なお、図中の吹き出しは、図４で示す送信機または受信機における「共有基底」などの各項目名に対応させた説明文である。

送信機100には共通鍵１(121)と共通鍵２(122)の２つの共通鍵、及び乱数発生器１(111)、乱数発生器２(112)、乱数発生器３(113)の３台の乱数発生器を用意する。但し、２つの共通鍵はひとつの共通鍵を２分割して利用することも可能であるし、３台の乱数発生器は１台の乱数発生器の出力を３分割して利用することも可能である。

【００４６】

乱数発生器１(111)は信号乱数の生成源である。揺らぎ（ノイズ）のために信号乱数列は受信時には誤りがあり、その誤りは基底の判定誤りとビット値の誤りに分類される。ビット誤りの対応には符号器141において誤り訂正符号化しておく。基底の誤り対応には共通鍵２(122)により決まるパリティ検査記号を利用する。パリティ検査記号は信号乱数列に無関係に決まるため、信号乱数列のパリティとパリティ検査記号とは一般に一致しない。

【００４７】

そこで、調整ビット挿入部126において調整ビットを付加して両パリティを一致させる

。共通鍵２はそのまま使うことも可能であるが、共通鍵２を種鍵として疑似乱数を発生させてそれをパリティ検査記号とすることも可能である。調整ビットが付加された信号乱数はバッファ131で待機する。ダミーは乱数発生器２(112)で生成し、バッファ132で待機する。ランダム基底は乱数発生器３(113)の出力で決定し、共通鍵１(121)で決まる共有基底と比較し、両基底が一致するかどうかで信号乱数を送信するかダミーを送信するかを決める。両基底が一致した場合はバッファ131に待機の信号乱数を送信するものとし、両基底が一致しなかった場合はバッファ132に待機のダミーを送信するものとする。

【００４８】

信号乱数及びダミーの値は揺らぎ光源151からの出力光に変調器161において重畳する。揺らぎ光源151は揺らぎ（ノイズ）を伴った光を生成する光源で、揺らぎの生成法としては、レーザーダイオード（ＬＤ）を閾値近傍で動作させることにより位相揺らぎを拡大する方法(特許文献１、及びＷＯ２０１１／０９９３２５を参照)、アンチスクイジングを利用した方法(特開２００８－００３３３９号公報を参照)等がある。また、揺らぎ源（ノイズ源）を別に用意し、ＬＤ光の出力に揺らぎ源の出力を重畳し疑似的に揺らいだ光源とすることも可能である(特許文献１、及びＷＯ２０１１／０９９３２５を参照)。揺らぎ源としては、乱数発生器の出力や熱揺らぎを利用する方法や、伝送用とは別のＬＤを用意し、そのＬＤ光の位相揺らぎを一旦受光しその電気的出力を揺らぎ源の出力として伝送用ＬＤの出力光に重畳する方法等が考えられる。尚、共通鍵１により共有基底を決定する方法は、共通鍵１をそのまま利用することも可能であるし、共通鍵を種鍵として疑似乱数を生成してそれを共有基底とすることも可能である。

【００４９】

信号乱数及びダミーが重畳された信号光は、伝送路201を通して受信機に伝送される。受信機ではまず検出器311により４値判定する。その判定結果に基づきランダム基底を決定する。受信機内には共通鍵１(321)を保持しており共有基底を決定する。共通鍵１(321)は送信機内の共通鍵１(121)と同じものであり、共有基底は送受信機双方で同一なものとなる。共有基底とランダム基底は比較され、各ビットの基底が一致するか、あるいは一致しないかに基づいて信号乱数とダミーに分離される。信号乱数列に関しては送信機内と同様な規則によりパリティを計算し、共通鍵２(322)で決まるパリティ検査記号を用いて検査する。検査結果が正しければ、検査を実施した一群の信号乱数列を正しく再現できたと判定する。検査結果が誤りであった場合は、検出器311での４値判定に誤りがあったとして、判定誤りがあったと考えられるビット近傍のひとつのビットに対して４値判定の結果を訂正してパリティ検査までの処理を繰り返す。この繰り返し処理を判定誤りのあったと考えられる領域のビットに対してひとつずつ順番に行い正しいランダム基底を見つける。これにより各ビットの基底が確定することになる。

【００５０】

基底が確定すれば２値判定により信号乱数を判定できる。但し、基底の判定に若干の判定誤りが残っていること、及び信号乱数の判定結果にも誤りがあることが予想される。そのために送信機側で符号器141により誤り訂正符号化してあった。受信機では復号器341によりその誤り訂正符号を復号する。

【００５１】

以上の処理により送信機内の乱数発生器１(111)の出力である信号乱数が受信機内で再現される。これにより送信機と受信機は同じ乱数を保持していることになる。本発明の目的は実データを安全に伝送することである。そのためには秘密鍵（暗号鍵）が必要であり、その秘密鍵生成のために上記の手順で乱数を送受信した。秘密鍵生成にあたっては送受信した乱数のビット数を減らす（情報量の縮小）処理を行う。これは秘密鍵の安全性を増強するためである（「秘匿性の増強」と呼ばれる）。例えば、00110の５ビットから１ビットの秘密鍵を生成する処理を考えることにする。一つの方法としては５ビットのパリティを取ることが考えられ、その場合は秘密鍵が“０”になる。秘密鍵生成の処理は送信機と受信機で同じ規則で行う。これにより送受信機内で同じ秘密鍵が生成される。

【００５２】

実データは送信機内の暗号器181において、秘密鍵生成部171で生成した秘密鍵により暗号化される。暗号化された実データは光送信部182において光信号に変換され、伝送路202を通して受信機300に伝送される。受信機では検出器381により電気信号に変換され、復号器382において秘密鍵生成部371で生成した秘密鍵を用いて実データの平文に変換される。以上で安全な通信が完了する。

【実施例３】

【００５３】

実施例２では、図４を用いて信号処理の例を述べた。そこでは、共有基底とランダム基底の一致不一致に従い信号乱数とダミーを分類した。

【００５４】

しかし、共有基底とランダム基底の比較の方法は図４に示す方法以外にもあり得る(特許文献１、及びＷＯ２０１１／０９９３２５を参照)。その例を示したのが図６である。この場合、共有基底とランダム基底の一致不一致に従い信号乱数とダミーを分類するのは同じであるが、不一致の場合にそのビットの共有基底を次ビットにおいて再利用する点が異なる。

【００５５】

図６では共有基底の第一ビットは“１”でランダム基底は“０”である。不一致なのでこのビットはダミーとする。第二ビットの決定に当たっては共有基底の第一ビット“１”を再度利用し、ランダム基底の第二ビット“１”と比較する。ここでは一致したので信号乱数とする。信号乱数であった場合には次のビットに進むに当たって共有基底も次に進むものとし、共有基底の第二ビット“０”とランダム基底の第三ビット“０”を比較する。両基底が一致したのでこのビットも信号乱数とする。以下同様に進める。

【００５６】

図６では図４の場合と同様に、信号乱数５ビットごとに１ビットの調整ビットを加えた例を示してある。

【００５７】

受信機においては実施例２と同様に送信器とは逆の処理を行い信号乱数とダミーを分類する。図６の右上段にその処理例を示す。受信機における４値判定に誤りがなければこのようにして信号乱数を再現できるが、４値判定に誤りがあれば図６の右下段の処理例に示すように信号乱数を再現できなくなる。図６の例では下線付きの第二ビットで判定を誤っている。この例では第二ビット以降、信号乱数の並びは正しい信号乱数の並びと全く異なる。誤りがあったと推定される近傍のビットに対して実施例２と同様にして１ビットずつ順番に、４値判定の結果の変更とパリティ検査とを繰り返し、ランダム基底を再現させる。

【実施例４】

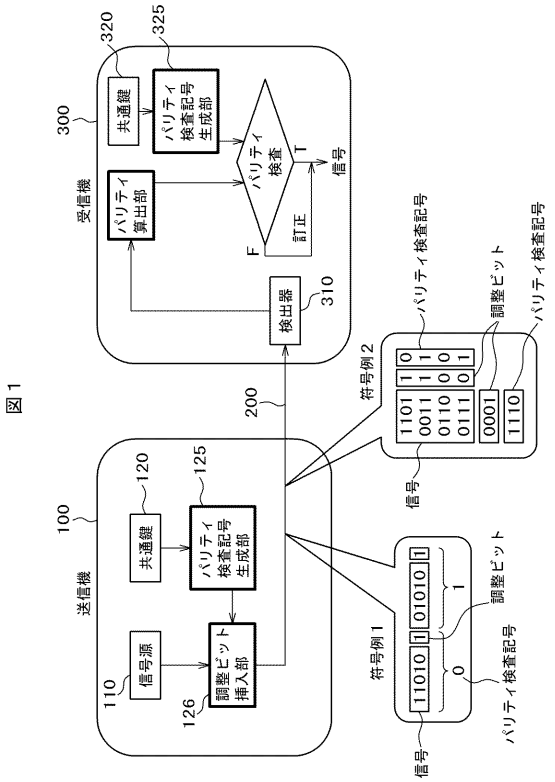
【００５８】

実施例２及び３においては共有基底とランダム基底の比較により信号乱数とダミーを決定した。この様な分類を行ったのは正規受信者に比べて不正受信者を不利にするためで共通鍵の利用法の一つである。実施例２及び３ではダミーを単純に破棄していたが、ダミーは信号乱数と同様に乱数でありこれも乱数データ群として利用することも可能である。即ち、実施例２及び３における信号乱数を信号乱数１とし、ダミーを信号乱数２として、２系列の信号乱数列として伝送することも可能である（ＷＯ２０１１／０９９３２５を参照）。その場合の信号処理例が図７及び図９である。それぞれ図４及び図６において「信号乱数」を「信号乱数１」に、「ダミー」を「信号乱数２」に書き換えたものになっている。図７及び９では信号乱数列が２つあるがパリティ検査記号は信号乱数列１に対してのみ用意した。これは信号乱数列１に対するパリティ検査記号だけで信号系列１と２に分類できるからである。但し、基底の訂正能力を向上させる目的や、このパリティ検査記号に、基底の判定誤りだけでなく信号乱数値に対する誤り訂正機能を持たせることを目的に信号乱数列２にもパリティ検査記号を用意する方法もあり得る。その場合の信号処理例を図８及び１０に示す。図８が図７の拡張であり、図１０が図９の拡張である。

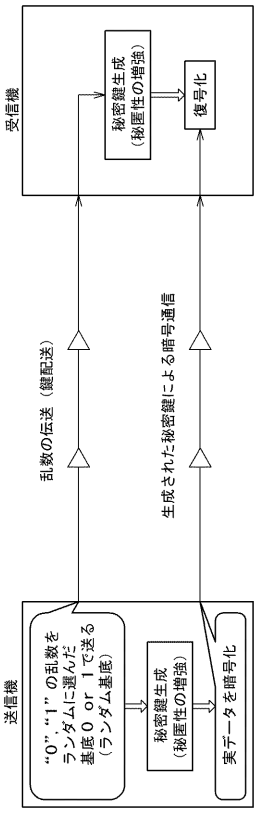
【００５９】
以上、共通鍵を利用してパリティ検査記号を決定する本発明に関して具体例を述べた。この方法は揺らぎを利用した安全な光通信法に適用した場合に効果が高いことが明らかであり、実施例２、３、４では「位相揺らぎを利用した安全な光通信法」を想定して実施例を述べた。但し、本発明はパリティ検査記号を共通鍵により決定するのがポイントであり、位相揺らぎを利用した安全な光通信法への適用に限定するものではない。また、信号重畳法は位相変調方式に限定されるものではなく、振幅変調方式や振幅変調と位相変調を組み合わせた方式等各種方式に適用可能である。但し、振幅変調方式の場合には対象となる揺らぎは振幅揺らぎになる。また、実施例では光通信を想定して述べたが無線通信等各種通信法にも適用可能である。

【符号の説明】
【００６０】
１００：送信機、
１１０：信号源、
１１１，１１２，１１３：乱数発生器、
１２０，１２１，１２２：共通鍵、
１２５：パリティ検査記号生成部、
１２６：調整ビット挿入部、
１３１，１３２：バッファ、
１４１：符号器、
１５１：揺らぎ光源、
１６１：変調器、
１７１：秘密鍵生成部、
１８１：暗号器、１８２：光送信部、
２００，２０１，２０２：伝送路、
３００：受信機、
３１０，３１１：検出器、
３２０，３２１，３２２：共通鍵、
３２５：パリティ検査記号生成部、
３４１：復号器、
３７１：秘密鍵生成部、
３８１：検出器、３８２：復号器。

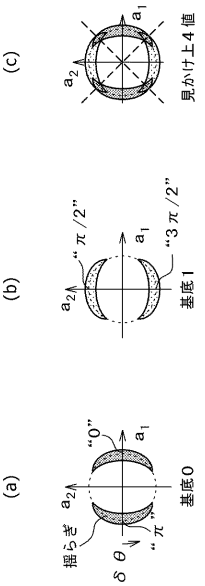
【図１】


送信機
100
信号源
110
共通鍵
120
調整ビット挿入部
126
パリティ検査記号生成部
125
200
符号例１
11010 0 01010 1
信号
0
1
調整ビット
パリティ検査記号
符号例２
1101 1 0
0011 1 1
0110 0 0
0111 0 1
信号
0001
1110
調整ビット
パリティ検査記号
受信機
300
共通鍵
320
パリティ検査記号生成部
325
パリティ算出部
パリティ検査
F
T
訂正
信号
検出器
310

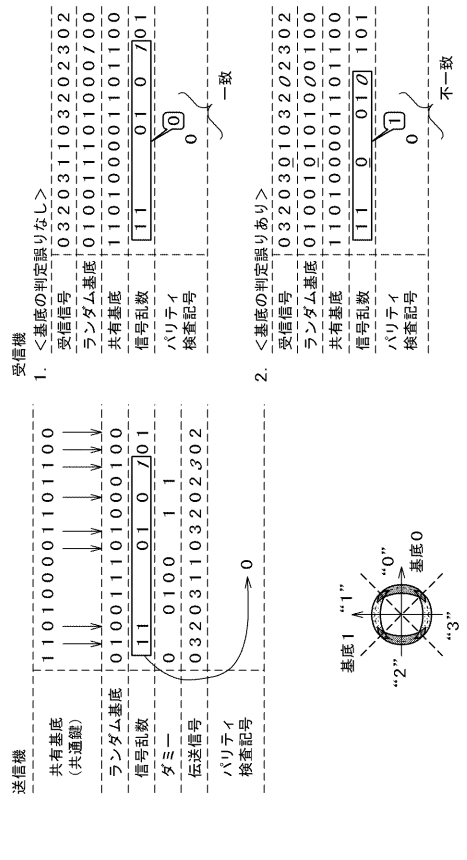
【図２】


送信機
“0”,“1”の乱数をランダムに選んだ基底０ or １で送る（ランダム基底）
秘密鍵生成（秘匿性の増強）
実データを暗号化
乱数の伝送（鍵配送）
生成された秘密鍵による暗号通信
受信機
秘密鍵生成（秘匿性の増強）
復号化

【図３】


(a)
揺らぎ
δθ
“0”
“π”
基底0
(b)
“π/2”
“3π/2”
基底1
(c)
見かけ上4値

【図４】


送信機
共有基底（共通鍵）
1101000011011100
ランダム基底
0100111010000100
信号乱数
11 01 01 7 01
ダミー
0 0100 1 1
伝送信号
0320311032023302
パリティ検査記号
0
受信機
1. <基底の判定誤りなし>
受信信号
0320311032023302
ランダム基底
0100111010000700
共有基底
1101000011011100
信号乱数
11 01 01 7 01
パリティ検査記号
0
0
一致
2. <基底の判定誤りあり>
受信信号
0320301032023302
ランダム基底
0100101010001100
共有基底
1101000011011100
信号乱数
11 0 01 101
パリティ検査記号
1
0
不一致
基底1
“1”
“0”
基底0
“2”
“3”

【図５】

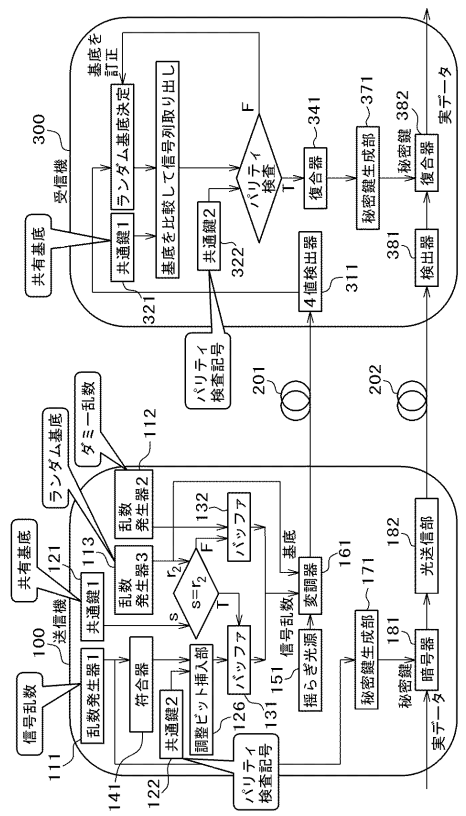


図5
送信機
受信機
信号乱数
乱数発生器1
符合器
共通鍵2
調整ビット挿入部
バッファ
揺らぎ光源
信号乱数
変調器
秘密鍵生成部
暗号器
光送信部
実データ
共有基底
ランダム基底
ダミー乱数
乱数発生器3
乱数発生器2
バッファ
共通鍵1
バリティ検査記号
4値検出器
検出器
復合器
秘密鍵
共通鍵1
ランダム基底決定
基底を訂正
基底を比較して信号列取り出し
共通鍵2
バリティ検査
実データ

【図６】

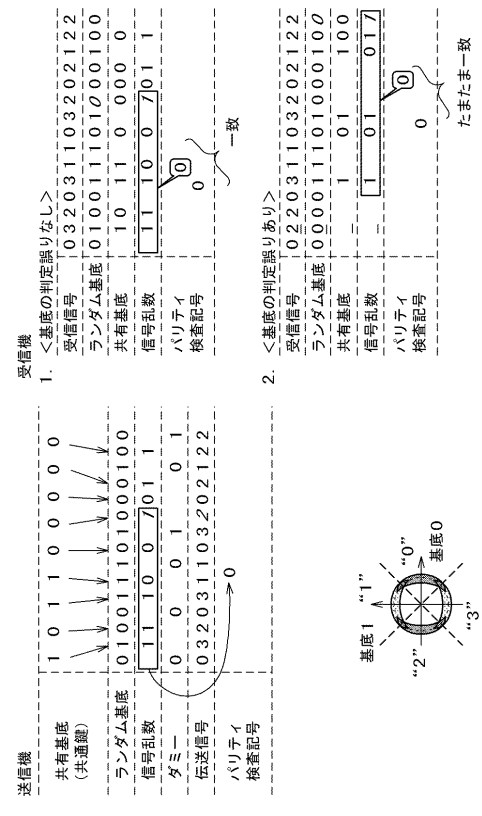


図6
送信機
受信機
1. <基底の判定誤りなし>
共有基底（共通鍵）
ランダム基底
信号乱数
ダミー
伝送信号
バリティ検査記号
受信信号
2. <基底の判定誤りあり>
一致
不一致
たまたま一致
基底1
基底0

【図７】

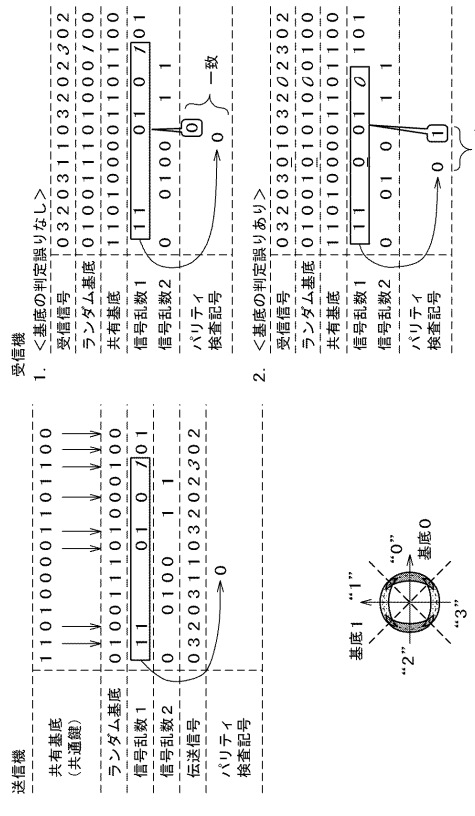


図7
送信機
受信機
1. <基底の判定誤りなし>
共有基底（共通鍵）
ランダム基底
信号乱数1
信号乱数2
伝送信号
バリティ検査記号
受信信号
2. <基底の判定誤りあり>
一致
不一致
基底1
基底0

【図８】

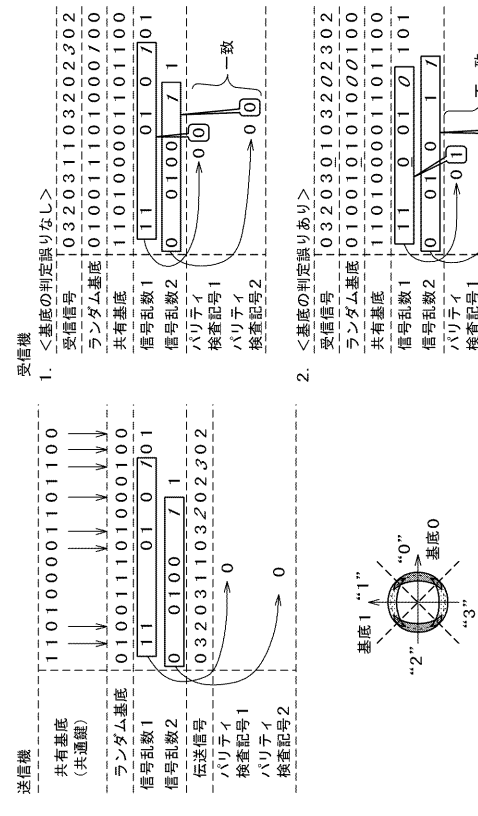


図8
送信機
受信機
1. <基底の判定誤りなし>
共有基底（共通鍵）
ランダム基底
信号乱数1
信号乱数2
伝送信号
バリティ検査記号1
バリティ検査記号2
受信信号
2. <基底の判定誤りあり>
一致
不一致
基底1
基底0

【図９】

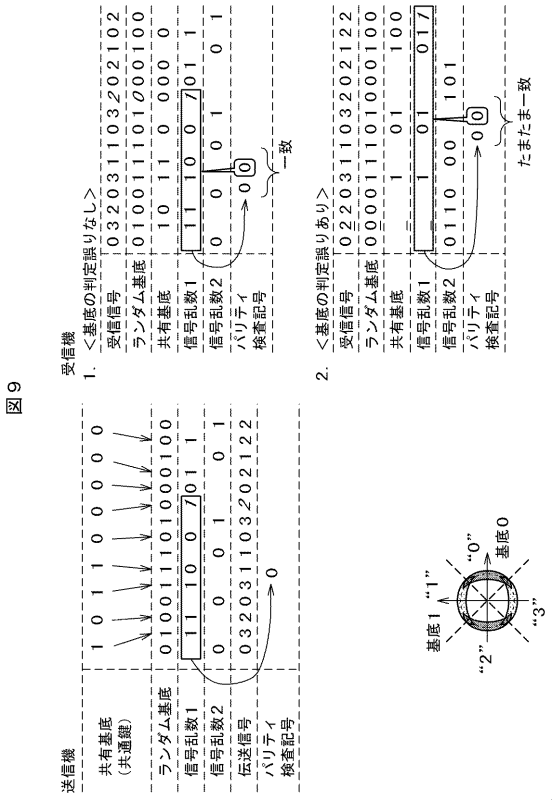


図９
送信機
共有基底
（共通鍵）
ランダム基底
信号乱数１
信号乱数２
伝送信号
パリティ
検査記号
受信機
１．＜基底の判定誤りなし＞
受信信号
ランダム基底
共有基底
信号乱数１
信号乱数２
パリティ
検査記号
一致
２．＜基底の判定誤りあり＞
受信信号
ランダム基底
共有基底
信号乱数１
信号乱数２
パリティ
検査記号
たまたま一致
基底１
“１”
“０”
基底０
“２”
“３”

【図１０】

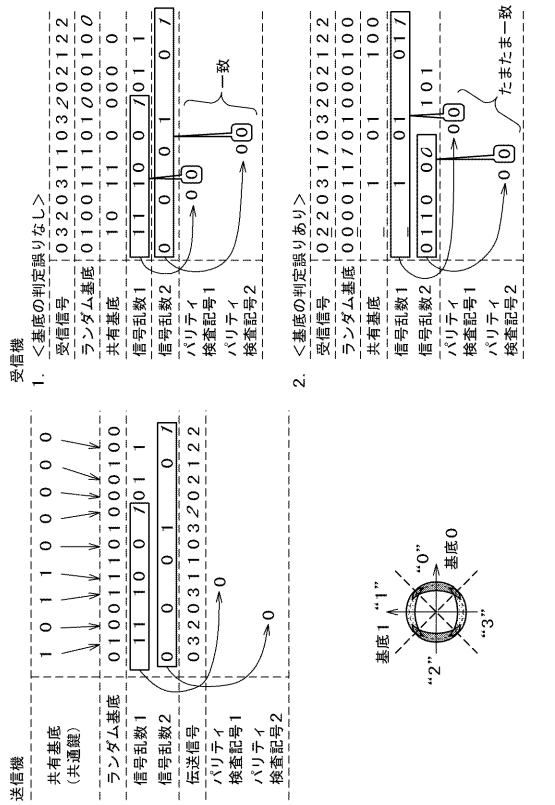


図１０
送信機
共有基底
（共通鍵）
ランダム基底
信号乱数１
信号乱数２
パリティ
検査記号１
パリティ
検査記号２
受信機
１．＜基底の判定誤りなし＞
受信信号
ランダム基底
共有基底
信号乱数１
信号乱数２
パリティ
検査記号１
パリティ
検査記号２
一致
２．＜基底の判定誤りあり＞
受信信号
ランダム基底
共有基底
信号乱数１
信号乱数２
パリティ
検査記号１
パリティ
検査記号２
たまたま一致
基底１
“１”
“０”
基底０
“２”
“３”

フロントページの続き

(56)参考文献 特開２０１１－１６６２９２（ＪＰ，Ａ）
特開２００７－１２９３８６（ＪＰ，Ａ）
特開２００６－０８０７２０（ＪＰ，Ａ）
米国特許出願公開第２００８／０２１９４４７（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１９０７１９（ＵＳ，Ａ１）
戸丸 辰也，“通信路揺らぎを利用した安全性向上”，２０１４年 暗号と情報セキュリティシンポジウム ＳＣＩＳ２０１４ ［ＣＤ－ＲＯＭ］，日本，電子情報通信学会情報セキュリティ研究専門委員会，２０１４年 1月２１日，１Ｆ１－４，ｐ．１－６

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／１２