(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
2012 年 4 月 12 日(12.04.2012)

PCT

(10) 国際公開番号
WO 2012/046463 A1

(51) 国際特許分類:
H04L 9/20 (2006.01)

(21) 国際出願番号: PCT/JP2011/054688

(22) 国際出願日: 2011 年 3 月 2 日(02.03.2011)

(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 2010-228259 2010 年 10 月 8 日(08.10.2010) JP

(71) 出願人 (米国を除く全ての指定国について): 学校法人玉川学園(**Tamagawa K-12 & University**) [JP/JP]; 〒1948610 東京都町田市玉川学園六丁目１番１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): 広田　修 (**HIROTA Osamu**) [JP/JP]; 〒2450061 神奈川県横浜市戸塚区汲沢６丁目２２番３０号 Kanagawa (JP).

(74) 代理人: 吉永　貴大, 外(**YOSHINAGA Takahiro** et al.); 〒1510064 東京都渋谷区上原１－３３－１４　ＭＫビル４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, CL, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, 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 (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, ML, MR, NE, SN, TD, TG).

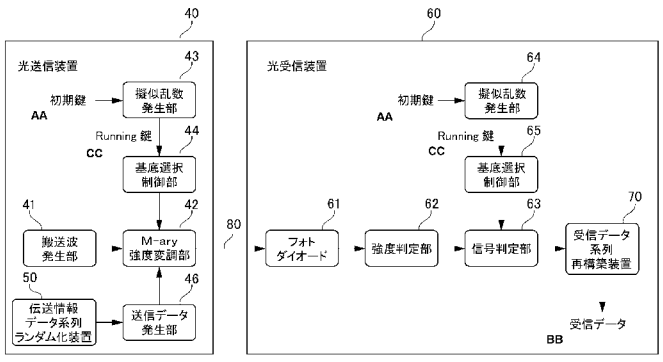
添付公開書類:
—　国際調査報告（条約第 21 条(3)）

WO 2012/046463 A1

(54) **Title**: OPTICAL TRANSMISSION DEVICE AND RECEIVING DEVICE FOR YUEN ENCRYPTION, OPTICAL TRANSMISSION METHOD AND RECEIVING METHOD FOR YUEN ENCRYPTION, AND ENCRYPTED COMMUNICATION SYSTEM

(54) 発明の名称 : Ｙｕｅｎ暗号用光送信装置及び受信装置、Ｙｕｅｎ暗号光送信方法及び受信方法、並びに暗号通信システム

[図3]



40 OPTICAL TRANSMISSION DEVICE
41 CARRIER WAVE GENERATOR UNIT
42 M-ARY INTENSITY MODULATOR UNIT
43, 64 PSUEDORANDOM NUMBER GENERATOR UNIT
44, 65 BASE SELECTION CONTROL UNIT
46 TRANSMISSION DATA GENERATOR UNIT
50 TRANSMISSION INFORMATION DATA SEQUENCE RANDOMIZER DEVICE
60 OPTICAL RECEIVING DEVICE
61 PHOTODIODE
62 INTENSITY ADJUDICATOR DEVICE
63 SIGNAL ADJUDICATOR DEVICE
70 RECEIVED DATA SEQUENCE REBUILDING DEVICE
AA INITIAL KEY
BB RECEIVED DATA
CC RUNNING KEY

(57) **Abstract**: [Problem] To provide an optical signal configuration method, encryption device, and encryption system whereby it is possible for an authorized communicating party to communicate long-distance with information-theoretic security ensured against a known-plaintext attack. [Solution] By adding a transmission information data sequence randomization device to this Yuen encrypted communications device, which divides transmission information into blocks, appends sequence numbers thereto, randomly switches the order of the blocks with a digitized signal of output of an electrical noise generator, and inputs same into a conventional Yuen encrypted optical transmitter transmission data generator, the relation between a known transmission information data sequence (plaintext) and an optical signal which is outputted from a transmitter is randomized, allowing forcibly making even a circumstance wherein a known-plaintext attack would be possible into a ciphertext-only attack, implementing information-theoretic security against a known-plaintext attack.

(57) 要約:

[続葉有]

【課題】既知平文攻撃に対する情報理論的安全性を確保し、正規通信者が長距離通信可能な光信号の構成法、暗号装置及び暗号システムを提供する。 【解決手段】本発明のＹｕｅｎ暗号通信装置は、伝送情報データをブロックに分割し、順序番号を付与して、電気雑音発生器の出力をデジタル化した信号によってブロックの順番をランダムに切り替えて、従来のＹｕｅｎ暗号光送信機の送信データ発生器に入力する、伝送情報データ系列ランダム化装置を付加することによって、既知の伝送情報データ系列（平文）と送信機から出力される光信号との関係をランダムにして、既知平文攻撃が可能な状況であっても強制的に暗号文単独攻撃の状況にすることを可能とし、既知平文攻撃に対する情報理論的安全性を実現する。

明　細　書

発明の名称 ：

Ｙｕｅｎ暗号用光送信装置及び受信装置、Ｙｕｅｎ暗号光送信方法及び受信方法、並びに暗号通信システム

技術分野

[0001] 本発明は、Ｙｕｅｎ暗号用光送信装置及び受信装置、Ｙｕｅｎ暗号光送信方法及び受信方法、並びに暗号通信システムに関する。

背景技術

[0002] 現代の情報通信ネットワークでは、第三者による通信文の盗聴を防ぐために、伝送する情報を数学的方法で攪乱する数理暗号が用いられている。近年、通信手段における信号系の物理現象を利用し、より高度な安全性の実現を目的とする物理暗号の開発が始められた。

[0003] 物理暗号の中でも、光信号を受信した際に不可避に発生する量子雑音によって暗号としての高度な安全性を実現する暗号は、Ｙｕｅｎ－２０００プロトコル（Ｙ－００と呼称）に基づくＹｕｅｎ暗号あるいは光通信量子暗号と呼ばれている。この暗号では、情報ビットを伝送するための２つの信号のセットを基底と呼び、基底を多数（Ｍ個）用意し、初期鍵を擬似乱数生成器によって伸長した擬似乱数列を用いて、不規則にその基底を選び、選ばれた基底に対応する光信号によって情報ビット（暗号学では平文と呼ぶ）を送信する。受信者は送信側と同期された送信者と同じ秘密鍵と擬似乱数生成器を用いて、１と０の２値の信号を識別する。

[0004] Ｙｕｅｎ暗号においては、鍵を知らない盗聴者はどの基底が用いられているか解らないので、２Ｍ個の信号を識別する必要がある。このとき、正規受信者の２値の識別の誤り特性はほぼゼロとなり、盗聴者の２Ｍ個の識別の誤り特性が極めて劣化するように信号と雑音効果を設計すると、盗聴者に対して高度な秘匿効果が得られる。このようにして秘匿効果を得ることを、通信方式と雑音効果に基づく安全性利得の生成原理と呼ぶ。

[0005] Ｙｕｅｎ暗号を実装する通信方式には、非特許文献１に開示されている光位相変調方式と、非特許文献２に開示されている光強度変調方式とが知られている。これらの方式では、基底に対応する光信号は１つの関係式にしたがって配置される。光位相変調方式では位相平面上で振幅Ａによる円周を信号数２Ｍで等間隔に分割した位置に配置される。光強度変調方式では、最大強度と最小強度との中間点を基準として２Ｍ等分あるいは最大から最小にかけて線形に間隔を小さくするなどの配置が用いられる。さらに用途によって種々の配置が提案されている。

[0006] 前述の信号配置は、量子雑音の効果が均等に出現するようにするための工夫である。盗聴者に対して秘密鍵に対する安全性（Ｑ）は次式によって簡易的に評価される（非特許文献２）。

[数1]

$$Q = \Gamma^{K/\log M} \qquad \cdots \quad (1)$$

式中、「は量子雑音に隠れる信号の数、Ｋは秘密鍵長、Ｍは基底数である。「＝Ｍのとき秘密鍵の可能性は観測数を増やしても全く減少しないので情報理論的安全という。位相変調方式では量子雑音は真空雑音と等価となるため極めて小さく、「を大きくする事が難しいが、強度変調方式での量子雑音は量子ショット雑音として出現するため量子雑音の量が大きく「を大きくすることが簡単にできるという特徴を有する。

[0007] 図１は、非特許文献２に記載の、従来技術に係る光強度変調を用いたＹｕｅｎ暗号の構成を表す図である。以下、図１を用いて、光強度変調方式によるＹｕｅｎ暗号装置の基本原理を説明する。

[0008] 図１において、従来の暗号通信装置は、光送信装置１０と光受信装置２０とが、光ファイバ等の光通信路３０で接続された構成である。光送信装置１０は、搬送波発生部１１と、Ｍ－ａｒｙ強度変調部１２と、擬似乱数発生部１３と、基底選択制御部１４と、送信データ発生部１５とを備える。光受信

装置２０はフォトダイオード２１と、強度判定部２２と、信号判定部２３、擬似乱数発生部２４と、基底選択制御部２５とを備える。光送信装置１０の擬似乱数発生部１３と光受信装置２０の擬似乱数発生部２４とは、構成及び機能が実質的に同一である。また、光送信装置１０の基底選択制御部１４と光受信装置２０の基底選択制御部２５とは、構成・機能が実質的に同一である。

[0009] 搬送波発生部１１は、例えばレーザ・ダイオードからなり、所定の光搬送波を出力する。送信データ発生部１５は、伝送すべき情報に基づいて情報「１」及び「０」で構成される送信データを発生する。擬似乱数発生部１３は、初期鍵Ｋに基づいて２進数擬似乱数列、すなわち２進数Ｒｕｎｎｉｎｇ鍵列を生成する。基底選択制御部１４は、この２進数Ｒｕｎｎｉｎｇ鍵列を、ｌｏｇＭビット毎にブロック分割し、その各ブロックに応じた１０進数Ｒｕｎｎｉｎｇ鍵に変換する。そして、基底選択制御部１４は、Ｒｕｎｎｉｎｇ鍵にしたがって基底群から１つの基底を選択し、基底情報としてＭ－ａｒｙ強度変調部１２に指示する。Ｍ－ａｒｙ強度変調部１２は、基底情報で指示されている基底に対応する光強度を用いて送信データで光搬送波を強度変調し、光通信路３０を介して光受信装置２０へ出力する。

[0010] フォトダイオード２１は、光通信路３０を介して光送信装置１０から出力される強度変調光信号を受信する。擬似乱数発生部２４は、初期鍵Ｋに基づいて２進数Ｒｕｎｎｉｎｇ鍵列を生成する。基底選択制御部２５は、この２進数Ｒｕｎｎｉｎｇ鍵列を、ｌｏｇＭビット毎にブロック分割し、その各ブロックに応じた１０進数Ｒｕｎｎｉｎｇ鍵に変換する。そして、基底選択制御部２５は、Ｒｕｎｎｉｎｇ鍵にしたがって基底群から１つの基底を選択し、基底情報として信号判定部２３に指示する。信号判定部２３は、基底選択制御部２５によって指示される基底情報に基づいて、受信信号をどのように判定するかを制御して、信号に含まれている情報「１」及び「０」を抽出し受信データとして出力する。具体的には、受信信号がしきい値より上あるいは下になるとき、１として判定する、あるいは０として判定する機能を有す

る。

[0011] 上述の従来のＹｕｅｎ暗号通信装置において、基底選択制御部１４及び２５で用いられる基底群、すなわち各基底に対応する光信号の配置は、暗号の強さを決定する重要な要素である。

先行技術文献

非特許文献

[0012] 非特許文献1：Ｅ．Ｃｏｒｎｄｏｒｆ，Ｃ．Ｌｉａｎｇ，Ｇ．Ｓ．Ｋａｎｔｅｒ，Ｐ．Ｋｕｍａｒ，Ｈ．Ｐ．Ｙｕｅｎ，“Ｑｕａｎｔｕｍ ｎｏｉｓｅ ｒａｎｄｏｍｉｚｅｄ ｄａｔａ ｅｎｃｒｙｐｔｉｏｎ ｆｏｒ ｗａｖｅｌｅｎｇｔｈ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅｘｅｄ ｆｉｂｅｒ ｏｐｔｉｃ”，Ｐｈｙｓｉｃａｌ Ｒｅｖｉｅｗ Ａ，ｖｏｌ－７１，０６２３２６，（２００５年）

非特許文献2：Ｏ．Ｈｉｒｏｔａ，Ｍ．Ｓｏｈｍａ，Ｍ．Ｆｕｓｅ，Ｋ．Ｋａｔｏ，“Ｑｕａｎｔｕｍ ｓｔｒｅａｍ ｃｉｐｈｅｒ ｂｙ Ｙｕｅｎ－２０００ ｐｒｏｔｏｃｏｌ：ｄｅｓｉｇｎ ａｎｄ ｅｘｐｅｒｉｍｅｎｔ ｂｙ ｉｎｔｅｎｓｉｔｙ ｍｏｄｕｌａｔｉｏｎ ｓｃｈｅｍｅ”，Ｐｈｙｓｉｃａｌ Ｒｅｖｉｅｗ Ａ，ｖｏｌ－７２，０２２３３５，（２００５年）

発明の概要

発明が解決しようとする課題

[0013] ところで、図２は、光強度変調によるＹｕｅｎ暗号の暗号文単独攻撃に対する情報理論的安全性を持つ光強度信号の配置の例である。以下、図２を用いて、光信号配置方法を説明する。まず、強度変調のダイナミックレンジを、最大強度S_{max}～最小強度S_{min}として設定する。この最大強度S_{max}と最小強度S_{min}との中心強度を、［（S_{max}＋S_{min}）／２］とする。各基底に対応する光信号は、高強度と低強度とで構成され、高強度は中心強度よりも高く、低強度は中心強度よりも低くなる規則で配置される。また、基底数M

は基底に対応する光信号群の中で、隣接する信号間（例えば、強度S_iと強度S_{i+1}との間）の距離（強度差）が、量子ショット雑音に埋没するに十分な数として決められる。例えば、図２で示すように、各信号強度を最大強度S_{max}から最小強度S_{min}まで順番にS_1，S_2，・・・・，S_{M-1}，S_M，S_{M+1}，・・・・，S_{2M}として、基底に対応する光信号のセットは｛S_1，S_{M+1}｝，｛S_2，S_{M+2}｝，・・・・のように規定する。なお、隣り合う基底間では、送信データの情報「１」を伝送する強度信号と、情報「０」を伝送する強度信号とが、反転するように配置設計されている。

[0014] 上述した従来のＹｕｅｎ暗号通信装置においては、正規受信者は、信号間距離が大きい２値の信号識別を行うことになるので誤りがほとんど無い。しかし、初期鍵Ｋを知らない盗聴者は、信号間距離の小さい２Ｍ値の信号識別のための受信方法に制限されるため、その受信データには量子ショット雑音により誤りが発生する。よって、盗聴者は、暗号文自体の情報を得ることができない。

[0015] このような仕組みはランダム・ストリーム暗号の一種であるが、量子ショット雑音によってランダム化されるため、そのランダム性を計算によって確定値に戻すことは不可能である。したがって、これらの理由から、Ｙｕｅｎ暗号は、従来の数学的な暗号システムに比べて高い安全性を持つ暗号を実現できると言える。

[0016] このように、Ｙｕｅｎ暗号は、通信システム自体が量子性の弱い従来の光通信で構成される。鍵を知らない盗聴者に対しては、量子ショット雑音によって情報が得られない工夫がなされていることに基づく極めて高い安全性を提供する。

[0017] 暗号技術において、暗号機構が情報理論的安全とは、無限の計算機を用いても解読できないことを意味する。従来の数理暗号では特殊な条件のもとで暗号文単独攻撃に対して情報理論的安全にできるが、既知平文攻撃に対しては原理的に情報理論的安全にはできない。

上記（図２）の信号配置を用いるＹｕｅｎ暗号は、暗号文単独攻撃に対し

て情報理論的安全性が保証され、既知平文攻撃に対しては部分的な安全性を持つことが証明されているが、十分とは言えない。Ｙｕｅｎ暗号は物理暗号の特徴として、既知平文攻撃を実施する多数の方法の中で、正規受信者と同じ方式の受信機を用いた最も原理的な既知平文攻撃を実施するには少なくとも１００億×１００億×１００億以上の回路要素が必要となる。この数値は将来にわたっても物理的に実現不可能である。このように天文学的な構成要素を持つ回路は実現不可能という条件の下では、その他の既知平文攻撃手法に対する完全な情報理論的安全性の実現可能性は否定されていない。

[0018] 本発明の目的は、暗号文単独攻撃に対する情報理論的安全性を有するＹｕｅｎ暗号に対して天文学的な構成要素を持つ回路は実現不可能という条件下で、既知平文攻撃に対する情報理論的安全性を実現する送信と受信法の構成法を提供することにある。

課題を解決するための手段

[0019] 本発明は、Ｙｕｅｎ暗号において、伝送しようとする情報データ（暗号学では平文という）をブロックにしてパケット化し、そのパケットの集団の順序をランダムに送信し、既知平文攻撃に対する情報理論的安全性を持つＹｕｅｎ暗号の実現に関する。

[0020] 本発明に係るＹｕｅｎ暗号光送信装置は、伝送する情報データ系列をブロックに分割し、そのブロックに番号を付加してパケット化し、そのパケットの順番をランダムにするための電気雑音発生器で構成される伝送情報データ系列ランダム化装置と、基底をランダム化するための擬似乱数発生部と、その出力系列を多数の基底に対応させる基底選択制御部と、選択された一つの基底と情報ビットに基づいた光強度信号を送信する強度光変調部とを備えるＹｕｅｎ暗号の基本構成要素を有する。

[0021] すなわち、本発明に係るＹｕｅｎ暗号光送信装置は、光強度変調方式によるＹ－００プロトコルを実装するＹｕｅｎ暗号光送信装置であって、光変調部への情報データ系列（入力情報）をブロックに分割し、そのブロックに番号を付加してパケット化し、そのパケットの順番を電気雑音発生器の出力系

列によってランダムに並べ替え、一つの系列としてＹｕｅｎ暗号の光変調部への入力系列とする仕組みを有し、初期鍵から擬似乱数列を発生する擬似乱数発生部と、多数の基底から構成される基底群を保持し、擬似乱数列に従って当該基底群から１つの基底を選択する基底選択制御部と、選択された１つの基底に対応する２つの光強度を用いて、伝送データに基づいた光変調信号を生成する強度光変調部とを備え、基底群を構成する全ての基底において、各基底に対応する２つの光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、中間点の上にある信号群の強度は、中間点から十分離れた光強度周辺に集中的に配置され、中間点の下にある信号群の強度は、中間点から十分離れた光強度付近に集中的に配置され、中間点の上にある信号群及び中間点の下にある信号群の強度が集中的に配置されるそれぞれの強度の範囲は、信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定されることを特徴とする。

[0022] また、本発明に係る光送信装置から出力される光信号を受信する光受信装置は、受信した光強度信号の最大受信強度と最小受信強度との中間点を識別しきい値として信号強度を判定して判定値を出力する強度判定部と、判定値に対して、光送信装置の初期鍵を用いて擬似乱数列を発生する擬似乱数発生部と、多数の基底から構成される基底群を保持し、擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御部と、基底選択制御部により選択された基底を用いて情報データの０と１を判定する信号判定部とで構成される基本的Ｙｕｅｎ暗号受信装置とそれによって復号された系列を送信側で設定されたブロック長にブロック化し、そのブロックに付加された番号順に並べ替える順序再構成部で構成される受信データ系列再構築装置を備えることを特徴とする。

[0023] すなわち、本発明の送信部は、光強度変調方式によるＹ－００プロトコルを用いるＹｕｅｎ暗号光送信方法であって、伝送される情報データ系列をブロックに分割し、順序を電気雑音発生器の出力によってランダムにし、それらを入力とし、１と０のデータを伝送する各基底に対応する２つの光信号の

強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、中間点の上にある信号群の強度は、中間点から十分離れた光強度周辺に集中的に配置され、中間点の下にある信号群の強度は、中間点から十分離れた光強度付近に集中的に配置され、中間点の上にある信号群及び中間点の下にある信号群の強度が集中的に配置されるそれぞれの強度の範囲は、信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定されることを特徴とする。

[0024] また、本発明の受信部は、Ｙｕｅｎ暗号光送信方法を用いて送信された光信号を受信するＹｕｅｎ暗号光受信装置であって、受信した光強度信号の最大受信強度と最小受信強度との中間点を識別しきい値として信号強度を判定して判定値を出力する強度判定部と、判定値に対して、光送信装置の初期鍵を用いて擬似乱数列を発生する擬似乱数発生部と、多数の基底から構成される基底群を保持し、擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御部と、基底選択制御部により選択された基底を用いて情報データの０と１を判定する信号判定部とによって復号された系列を送信側で設定されたブロック長にブロック化し、そのブロックに付加された番号順に並べ替える順序再構成部、を含む。

発明の効果

[0025] 本発明によれば、従来のＹｕｅｎ暗号が暗号文単独攻撃に対して情報理論的安全性を有していれば、天文学的規模の構成要素を持つ攻撃装置が実現できないとする制約の下では、既知平文攻撃に対する情報理論的安全性を持つＹｕｅｎ暗号の実現を低コストで提供できる。

図面の簡単な説明

[0026] [図1]従来技術に係る、光強度変調を用いたＹｕｅｎ暗号の構成を表す図である。

[図2]光強度変調を用いたＹｕｅｎ暗号の暗号文単独攻撃に対する情報理論的安全性を持つ光強度信号の配置実施例を表す図である。

[図3]本発明の実施形態に係る、Ｙｕｅｎ暗号を用いる暗号通信装置の構成を

表す図である。

[図4]本発明の実施形態に係る、伝送情報データ系列ランダム化装置５０の構成を表す図である。

[図5]本発明の実施形態に係る、受信データ系列再構築装置７０の構成を表す図である。

発明を実施するための形態

[0027] 以下、本発明を実施するための形態（以下、実施形態）について詳細に説明する。

[0028] 図３は、本発明の実施形態に係る、Ｙｕｅｎ暗号を用いる暗号通信装置の構成を表す図である。図３に示すように、本発明に係る光送信装置４０と光受信装置６０とを、光ファイバ等の光通信路８０を介して接続し、本発明に係る送信及び受信方法を実施することにより、本発明に係る暗号通信システムを構成することができる。

[0029] 具体的には、本実施形態に係るＹｕｅｎ暗号通信システムは、光送信装置４０、光受信装置６０及び光通信路８０を備える。

[0030] 光送信装置４０は、入力情報を一以上のブロックに分割し、該ブロックに番号を付加してパケット化し、パケットの順番を電気雑音発生器（電気雑音発生部５４、図４）の出力系列を用いてランダム化して並べ替えた送信情報を生成する伝送情報データ系列ランダム化装置５０と、初期鍵から擬似乱数列を発生する送信機擬似乱数発生部としての擬似乱数発生部４３と、多数の基底から構成される基底群を保持し、擬似乱数列にしたがって当該基底群から１つの基底を選択する送信機基底選択制御部としての基底選択制御部４４と、選択された１つの基底に対応する２つの光強度を用いて、送信情報に基づいた光変調信号を生成する強度光変調部としてのＭ－ａｒｙ強度変調部４２とを備え、基底群を構成する全ての基底において、各基底に対応する２つの光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、中間点の上にある信号群の強度は、中間点から十分離れた光強度周辺に集中的に配置され、中間点の下にある信号群の強度は、中間点から十分離れた

光強度付近に集中的に配置され、中間点の上にある信号群及び中間点の下にある信号群の強度が集中的に配置されるそれぞれの強度の範囲は、信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定される。搬送波発生部４１の動作は、図１に示した搬送波発生部１１と同等である。

[0031] このように、本実施形態に係る光送信装置４０は、送信データ発生部４６への入力前に、本発明に係わる伝送情報データ系列ランダム化装置５０により、伝送される情報データをランダム化し、それを送信データ発生部４６に入力して、既知の平文と光出力の関係をランダムにする。これにより、既知の平文と暗号文の関係がランダム化される。したがって、既知平文攻撃が可能な状況でありながら、暗号文単独の状況を作り出すことによって、既知平文攻撃に対する情報理論的安全性を実現できる。

[0032] また、本実施形態に係る光受信装置６０においては、図３のフォトダイオード６１を介して光信号を受信する。フォトダイオード６１の動作は、図１に示したフォトダイオード２１と同等である。光受信装置６０は、最大強度と最小強度の中間点の信号強度に対応する受信信号強度にしきい値を設定し、該しきい値に対して上あるいは下の情報を出力する強度判定部６２と、送信装置で使用した同じ初期鍵と擬似乱数発生部６４からの出力系列によって、基底選択制御部６５を経由して情報ビットの０あるいは１を判定する信号判定部６３とからなり、その出力系列を受信データ系列再構築装置７０によって元の情報データに戻すことによって、暗号通信が完了する。

[0033] 図４に、本発明に係る伝送情報データ系列ランダム化装置５０の構成を示す。本発明のＹｕｅｎ暗号光送信装置は、基本的に図１に示した光送信装置１０と、伝送情報データ系列ランダム化装置５０とによって構成できる。すなわち、本発明に係るＹｕｅｎ暗号の光送信装置４０（図３）は、伝送情報データ系列ランダム化装置５０を、従来のＹｕｅｎ暗号の光送信装置１０（図１）の送信データ発生部１５の入力に接続することによって構成される。

[0034] 図５に、本発明に係る受信データ系列再構築装置７０の構成を示す。本発

明に係る光受信装置６０（図３）は、図１に示した従来のＹｕｅｎ暗号の光受信装置２０の信号判定部の出力に、受信データ系列再構築装置７０を接続することによって構成される。

[0035] 本発明は、光送信装置１０の送信データ発生部の入力の前処理として、情報データ系列のブロック化とその順序のランダム化に特徴があり、そのランダム化によって、情報データと暗号化された光信号の関係を独立にし、既知平文攻撃に対する情報理論的安全性を実現するという特徴を有している。以下に、本発明の特徴的なデータのランダム化ついて図面を参照しながら説明する。

[0036] （情報データ系列のランダム化）

図４に示した伝送情報データ系列ランダム化装置５０の構成を用いて、情報データ系列のランダム化を説明する。本発明の実施形態では以下のように情報データ系列をランダム化する。

[0037] 伝送すべきデータ系列（入力情報）は、伝送情報データ入力部５１に入力される。次いで、データ系列ブロック化部５２は、該データ系列を一連のビット系列としてブロック化する。例えば、ｍビット毎のブロック化を行う。次いで、順序番号付加部５３は、このブロックの集合に順序番号に対応するビット系列を付加する。電気雑音発生部５４は電気的な雑音を発生し、この雑音はデジタル化部５５において数値情報に変換される。順序変換部５６は、順序番号を付加されたブロックの順番を、雑音に基づく数値情報を用いてランダム化する。したがって、順序変換部５６の出力は、入力された情報データ系列に対してブロック化の順番がランダムなビット系列である。この出力は、Ｙｕｅｎ暗号光送信装置の送信データ発生部に順次送られる。

[0038] 本発明の実施形態に係る情報データ系列のランダム化により、情報データ系列が既知であっても、光送信装置から出力される光信号は、基底を選択する擬似乱数発生部の出力系列のランダム性とランダム化された情報データ系列との両方によって撹拌されたものになる。

[0039] さらに、基底群を構成する全ての基底において、各基底に対応する２つの

光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、中間点の上にある信号群の強度は、中間点から十分離れた光強度周辺に集中的に配置され、中間点の下にある信号群の強度は、中間点から十分離れた光強度付近に集中的に配置され、中間点の上にある信号群及び中間点の下にある信号群の強度が集中的に配置されるそれぞれの強度の範囲は、信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定されていれば、盗聴者の受信機では上半面にある信号は全く識別できない。また、同じように下半面にある信号も識別できない。したがって、式（１）において「＝Ｍとなり秘密鍵の可能性は、盗聴者に対して

[数2]

$$Q = M^{K/\log M} \qquad \cdots \quad (2)$$

となり、いくら既知の平文に対応する暗号文を観測しても鍵の候補が減らないことになる。

すなわち、既知平文攻撃が可能な状況でありながら、平文にあたる情報データと暗号文の対応関係がランダムになり、暗号文単独攻撃と同じ状況になる。上記システムは暗号文単独攻撃に対して情報理論的安全性を持つので、このシステムは既知平文攻撃に対しても完全な情報理論的安全性を持つことになる。

[0040] 図５に示した、本発明の実施形態に係る情報データ系列のランダム化を用いたＹｕｅｎ暗号の光受信装置における受信データ系列再構築装置７０の構成を用いて、情報データ系列のランダム化を用いたＹｕｅｎ暗号のための光受信装置を説明する。

[0041] 本実施形態の受信データ系列再構築装置７０において、従来のＹｕｅｎ暗号の受信機能によって誤り無く復号された情報データ系列は、送信側でのブロック単位で順序番号判定部７１に入力され、その順序番号判定結果に基づいて、順序再構成部７２において元の順番に戻される。これにより、本実施

形態に係る光受信装置においては、送信側での本発明に係わるランダム化の影響のない受信データが得られる。

[0042] 以上のように、本実施形態に係る暗号通信のための光送信装置と光受信装置によれば、既知平文攻撃に対する情報理論的安全性を確保し、正規通信者の通信可能距離をより長距離とすることが可能な、通信能力を高めた光信号の構成法、送信法、受信法、光送信装置、光受信装置、及び暗号通信システムを低コストで提供することができる。

[0043] 以上、実施形態を用いて本発明を説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されないことは言うまでもない。上記実施形態に、多様な変更または改良を加えることが可能であることが当業者に明らかである。またその様な変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

産業上の利用可能性

[0044] 本発明は、クラウド・コンピューテイング・システムに必須となるデータセンター間の超安全光通信網を実現するための基幹技術となり得る。

符号の説明

[0045] １０　光送信装置

１１、４１　搬送波発生部

１２、４２　Ｍ－ａｒｙ強度変調部

１３、２４、４３、６４　擬似乱数発生部

１４、２５、４４、６５　基底選択制御部

１５、４６　送信データ発生部

２０　光受信装置

２１、６１　フォトダイオード

２２、６２　強度判定部

２３、６３　信号判定部

３０、８０　光通信路

４０　光送信装置（伝送情報データランダム化付き）

５０　伝送情報データ系列ランダム化装置

５１　伝送情報データ入力部

５２　データ系列ブロック化部

５３　順序番号付加部

５４　電気雑音発生部

５５　デジタル化部

５６　順序変換部

６０　光受信装置（伝送情報データランダム化解除付き）

７０　受信データ系列再構築装置

７１　順序番号判定部

７２　順序再構成部

請求の範囲

[請求項1] 光強度変調方式によるＹ－００プロトコルを実装するＹｕｅｎ暗号光送信装置であって、

入力情報を一以上のブロックに分割し、前記ブロックに番号を付加してパケット化し、前記パケットの順番を電気雑音発生器の出力系列を用いてランダム化して並べ替えて送信情報を生成する伝送情報データ系列ランダム化装置と、

初期鍵から擬似乱数列を発生する擬似乱数発生部と、

多数の基底から構成される基底群を保持し、前記擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御部と、

前記選択された１つの基底に対応する２つの光強度を用いて、前記送信情報に基づいた光変調信号を生成する強度光変調部とを備え、

前記基底群を構成する全ての基底において、各基底に対応する２つの光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、

前記中間点の上にある信号群の強度は、前記中間点から十分離れた光強度周辺に集中的に配置され、

前記中間点の下にある信号群の強度は、前記中間点から十分離れた光強度付近に集中的に配置され、

前記中間点の上にある前記信号群及び前記中間点の下にある前記信号群の強度が集中的に配置されるそれぞれの強度の範囲は、前記信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定されることを特徴とする

Ｙｕｅｎ暗号光送信装置。

[請求項2] 請求項１に記載の光送信装置から出力される光信号を受信する光受信装置であって、

受信した２値光強度信号の最大受信強度と最小受信強度との中間点を識別しきい値として信号強度を判定して判定値を出力する強度判定

部と、

前記判定値に対して、前記光送信装置の前記初期鍵を用いて擬似乱数列を発生する擬似乱数発生部と、

多数の基底から構成される基底群を保持し、前記擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御部と、

前記基底選択制御部により選択された前記基底を用いて情報ビットの０と１を判定する信号判定部と、

前記信号判定部により判定された前記情報ビットからなるデータ系列を前記光送信装置において設定されたブロックの長さにブロック化し、前記ブロックに付加された番号の順序に再構成した受信データ系列を生成する受信データ系列再構築装置と、を備えることを特徴とする

Ｙｕｅｎ暗号光受信装置。

[請求項3] 光強度変調方式によるＹ－００プロトコルを用いるＹｕｅｎ暗号光送信方法であって、

入力情報を一以上のブロックに分割し、前記ブロックに番号を付加してパケット化し、前記パケットの順番を電気雑音発生器の出力系列を用いてランダム化して並べ替えて送信情報を生成する伝送情報データ系列ランダム化処理と、

初期鍵から擬似乱数列を発生する擬似乱数発生処理と、

多数の基底から構成される基底群を保持し、前記擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御処理と、

前記選択された１つの基底に対応する２つの光強度を用いて、前記送信情報に基づいた光変調信号を生成する強度光変調処理とを含み、

前記基底群を構成する全ての基底において、各基底に対応する２つの光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、

前記中間点の上にある信号群の強度は、前記中間点から十分離れた

光強度周辺に集中的に配置され、

前記中間点の下にある信号群の強度は、前記中間点から十分離れた光強度付近に集中的に配置され、

前記中間点の上にある前記信号群及び前記中間点の下にある前記信号群の強度が集中的に配置されるそれぞれの強度の範囲は、前記信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定されることを特徴とする、

Ｙｕｅｎ暗号光送信方法。

[請求項4] 請求項３に記載のＹｕｅｎ暗号光送信方法を用いて送信された光信号を受信するＹｕｅｎ暗号光受信方法であって、

受信した２値光強度信号の最大受信強度と最小受信強度との中間点を識別しきい値として信号強度を判定して判定値を出力する強度判定処理と、

前記判定値に対して、前記光送信装置の前記初期鍵を用いて擬似乱数列を発生する擬似乱数発生処理と、多数の基底から構成される基底群を保持し、前記擬似乱数列にしたがって当該基底群から１つの基底を選択する基底選択制御処理と、

前記基底選択制御部により選択された前記基底を用いて情報ビットの０と１を判定する信号判定処理と、

前記信号判定処理により判定された前記情報ビットからなるデータ系列を前記光送信方法において設定されたブロックの長さにブロック化し、前記ブロックに付加された番号の順序に再構成した受信データ系列を生成する受信データ系列再構築処理と、を含む

Ｙｕｅｎ暗号光受信方法。

[請求項5] 光強度変調方式によるＹ－００プロトコルを実装するＹｕｅｎ暗号通信システムであって、前記Ｙｕｅｎ暗号通信システムは、Ｙｕｅｎ暗号光送信装置と、Ｙｕｅｎ暗号光受信装置とを有し、前記Ｙｕｅｎ暗号光送信装置は、

入力情報を一以上のブロックに分割し、前記ブロックに番号を付加してパケット化し、前記パケットの順番を電気雑音発生器の出力系列を用いてランダム化して並べ替えて送信情報を生成する伝送情報データ系列ランダム化装置と、

初期鍵から擬似乱数列を発生する送信機擬似乱数発生部と、

多数の基底から構成される基底群を保持し、前記擬似乱数列にしたがって当該基底群から１つの基底を選択する送信機基底選択制御部と、

前記選択された１つの基底に対応する２つの光強度を用いて、前記送信情報に基づいた光変調信号を生成する強度光変調部とを備え、

前記基底群を構成する全ての基底において、各基底に対応する２つの光信号の強度は、最大強度と最小強度の中間点を挟んで上と下に値を持ち、

前記中間点の上にある信号群の強度は、前記中間点から十分離れた光強度周辺に集中的に配置され、

前記中間点の下にある信号群の強度は、前記中間点から十分離れた光強度付近に集中的に配置され、

前記中間点の上にある前記信号群及び前記中間点の下にある前記信号群の強度が集中的に配置されるそれぞれの強度の範囲は、前記信号群の強度近傍のエネルギーに比例して出現する量子ショット雑音によって全て隠されるように設定され、

前記Ｙｕｅｎ暗号光受信装置は、

受信した２値光強度信号の最大受信強度と最小受信強度との中間点を識別しきい値として信号強度を判定して判定値を出力する強度判定部と、

前記判定値に対して、前記光送信装置の前記初期鍵を用いて擬似乱数列を発生する受信機擬似乱数発生部と、

多数の基底から構成される基底群を保持し、前記擬似乱数列にした

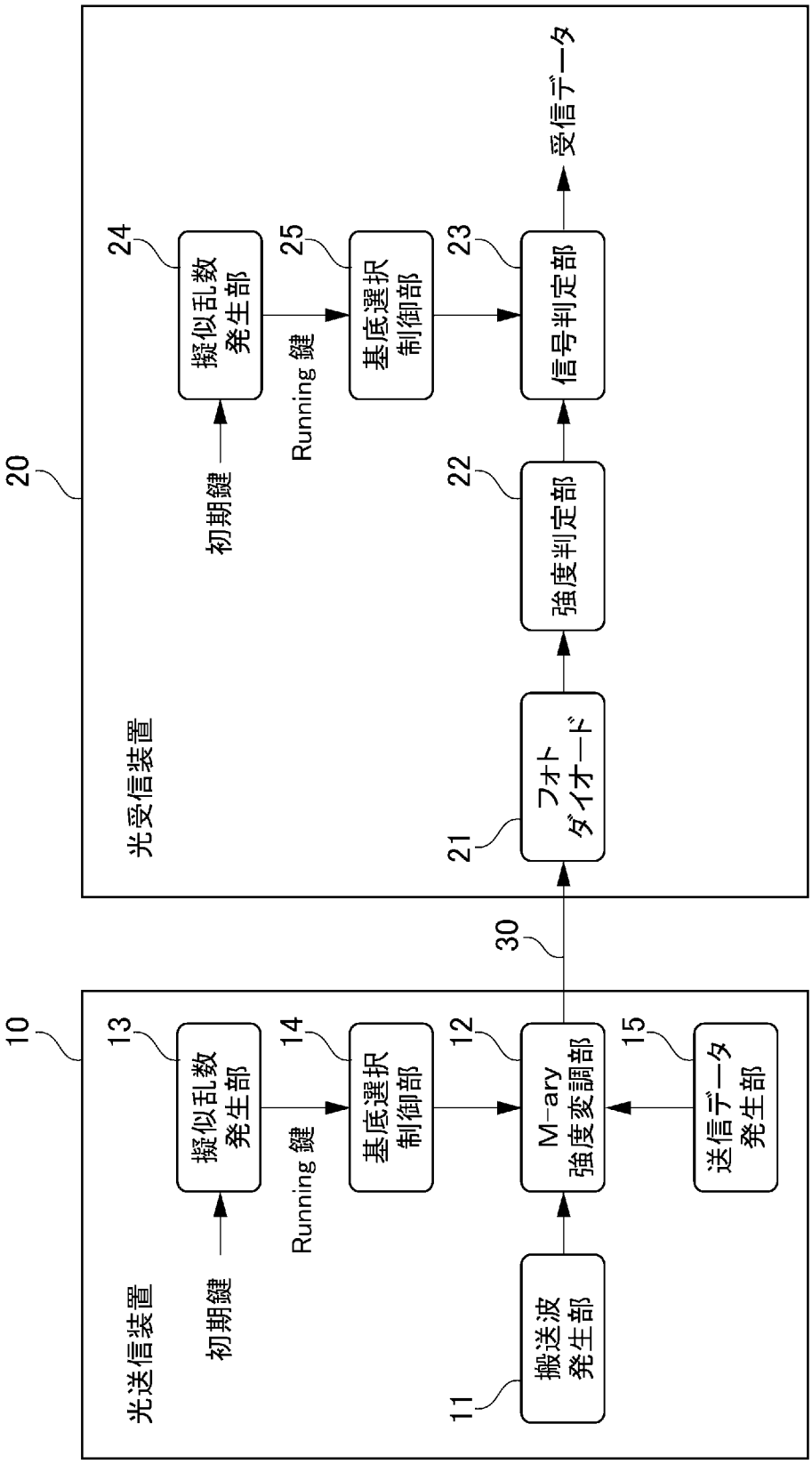
がって当該基底群から１つの基底を選択する受信機基底選択制御部と、

前記受信機基底選択制御部により選択された前記基底を用いて情報ビットの０と１を判定する信号判定部と、

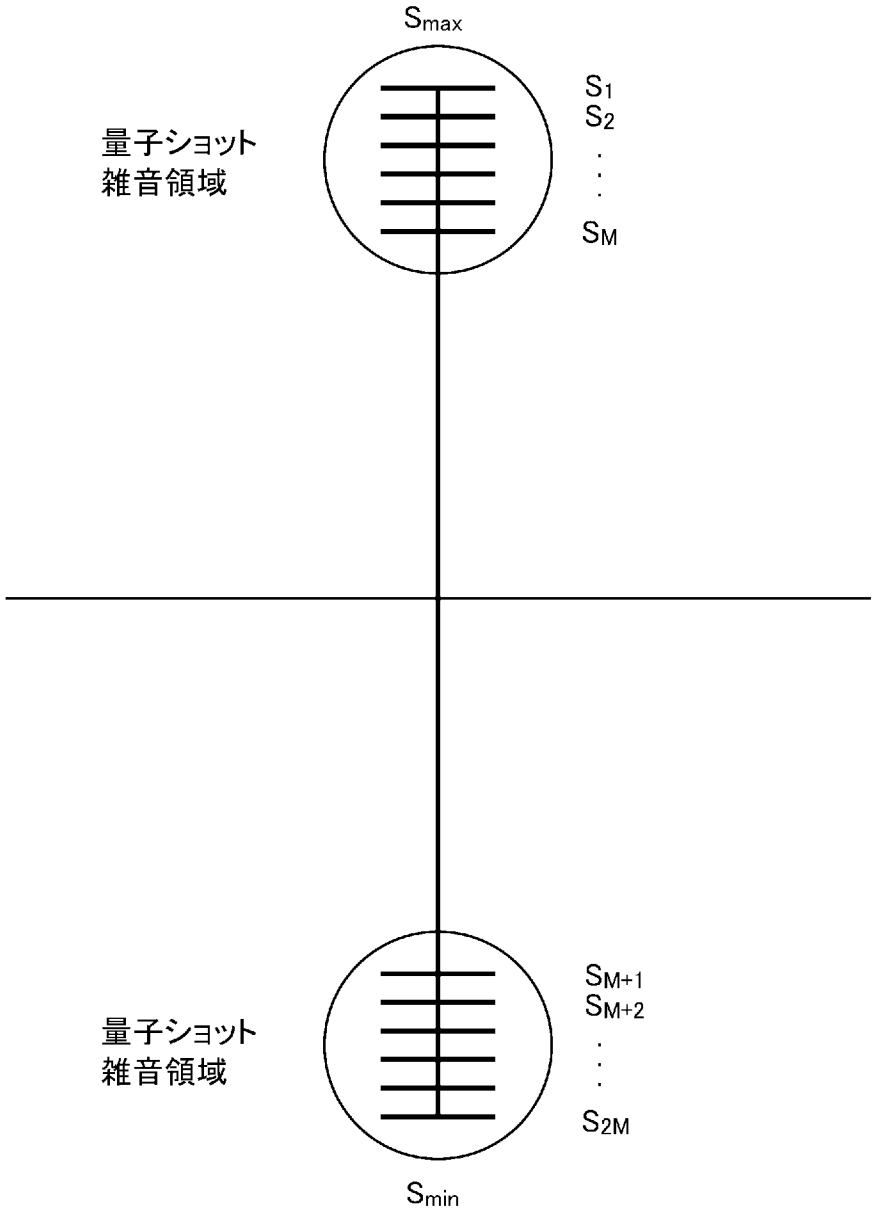
前記信号判定部により判定された前記情報ビットからなるデータ系列を前記Ｙｕｅｎ暗号光送信装置において設定された前記ブロックの長さにブロック化し、前記ブロックに付加された前記番号の順序に再構成した受信データ系列を生成する受信データ系列再構築装置と、を備える、

Ｙｕｅｎ暗号通信システム。

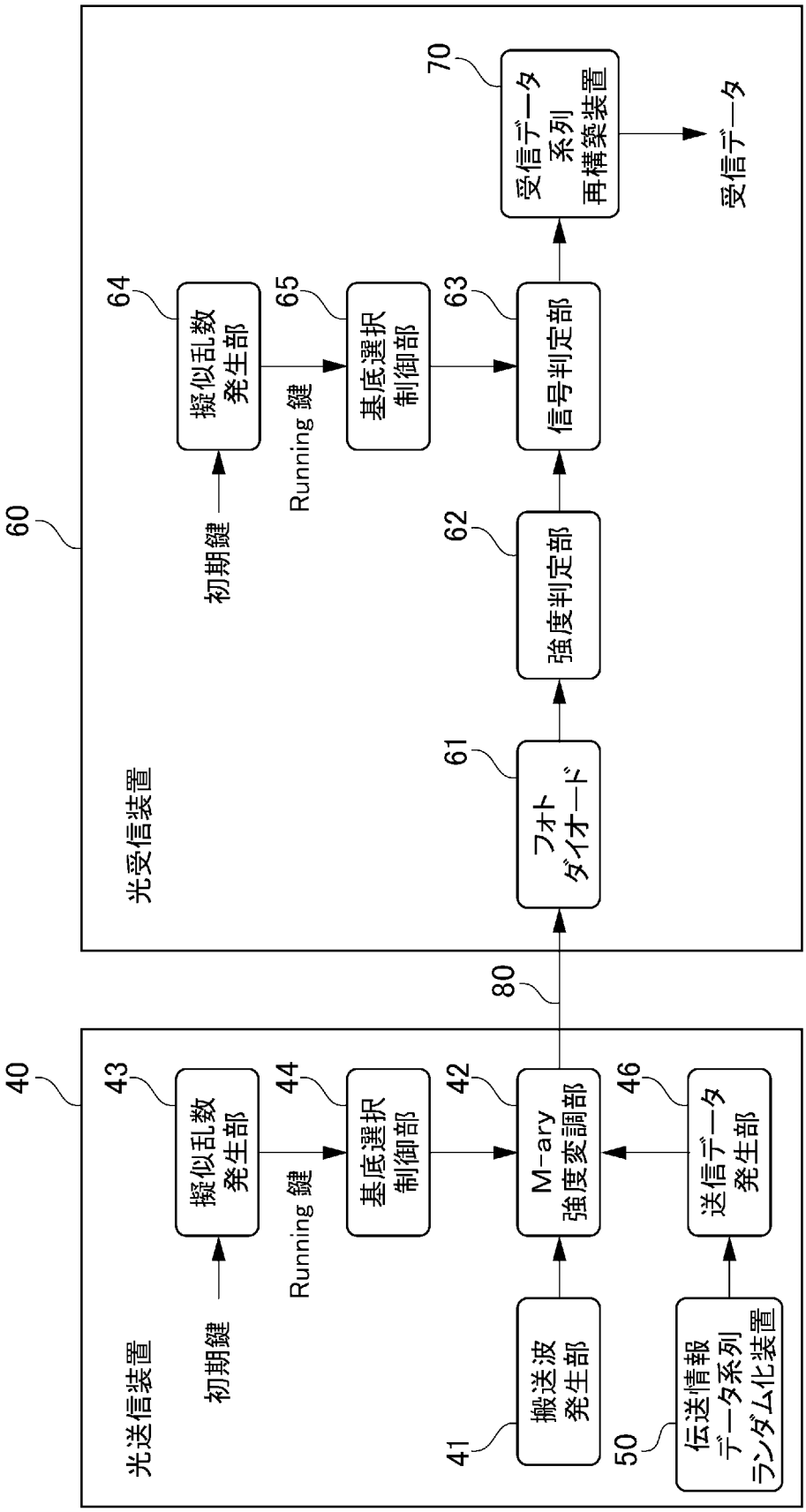
[図1]


光送信装置
10
擬似乱数発生部
13
初期鍵
Running 鍵
基底選択制御部
14
M-ary強度変調部
12
搬送波発生部
11
送信データ発生部
15
30
光受信装置
20
フォトダイオード
21
強度判定部
22
信号判定部
23
基底選択制御部
25
擬似乱数発生部
24
初期鍵
Running 鍵
受信データ

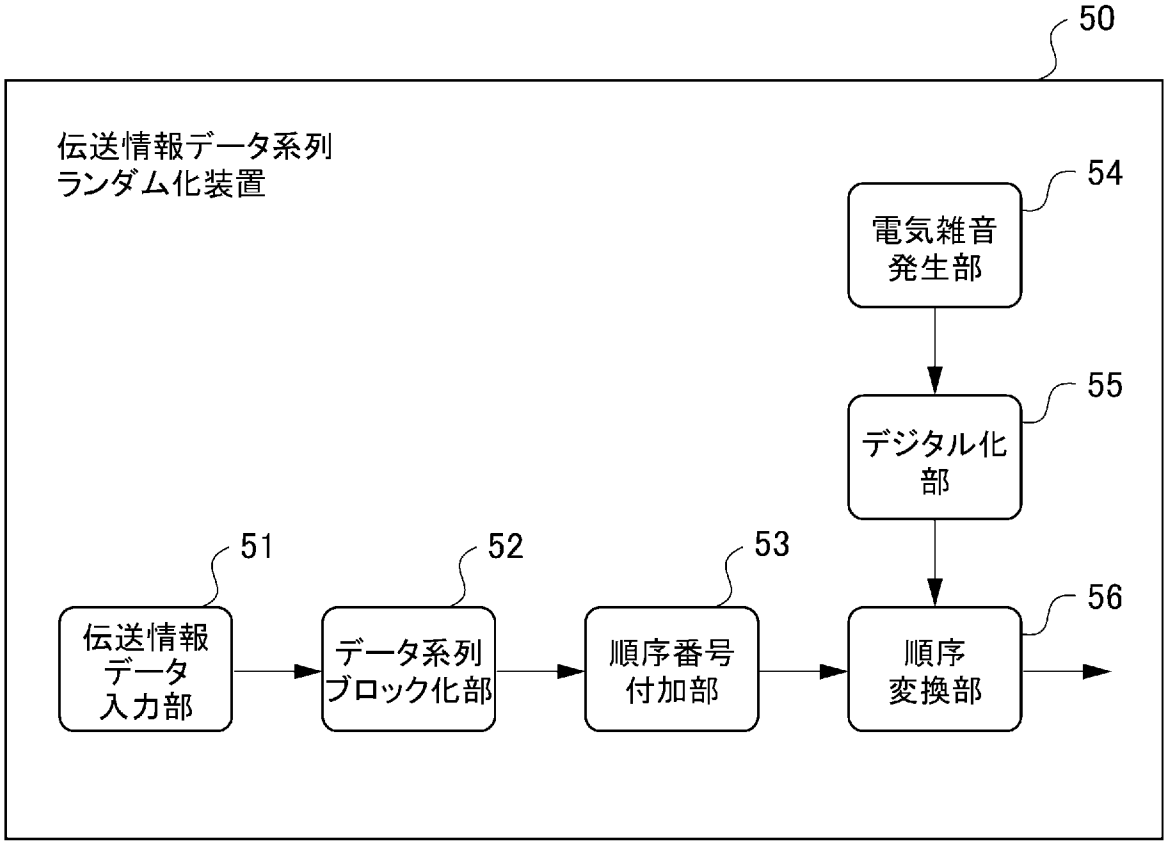
[図2]



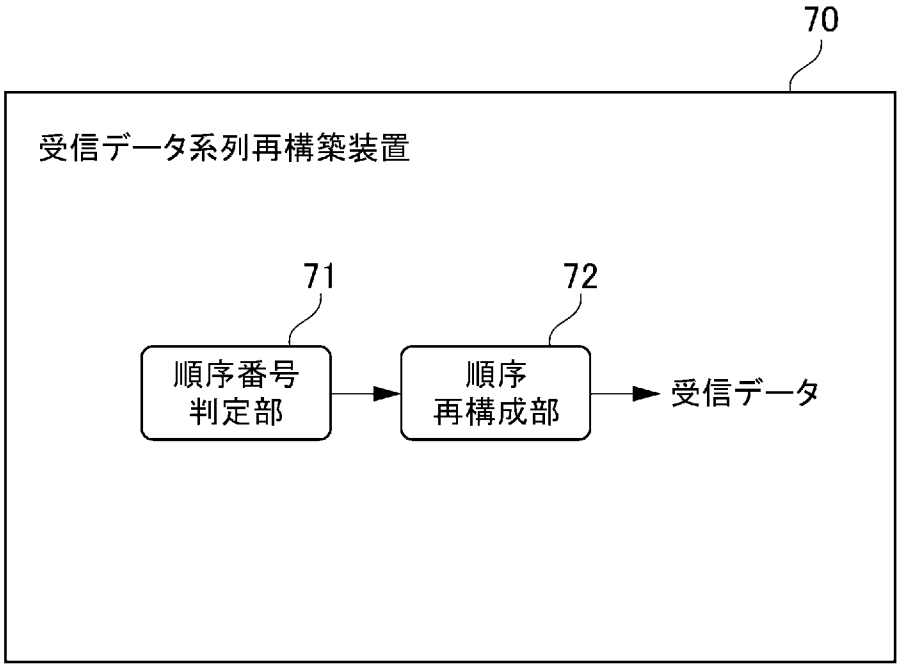
[図3]


光送信装置
40
擬似乱数発生部
43
初期鍵
Running 鍵
基底選択制御部
44
M-ary強度変調部
42
搬送波発生部
41
送信データ発生部
46
伝送情報データ系列ランダム化装置
50
80
光受信装置
60
フォトダイオード
61
強度判定部
62
信号判定部
63
基底選択制御部
65
擬似乱数発生部
64
初期鍵
Running 鍵
受信データ系列再構築装置
70
受信データ

[図4]


50
伝送情報データ系列
ランダム化装置
54
電気雑音
発生部
55
デジタル化
部
51
52
53
56
伝送情報
データ
入力部
データ系列
ブロック化部
順序番号
付加部
順序
変換部

[図5]


70
受信データ系列再構築装置
71
72
順序番号
判定部
順序
再構成部
受信データ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/054688

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/20(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)
H04L9/20

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII) Y-00

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ohhata, K. et al., 10-Gb/s Optical Transceiver Using the Yuen 2000 Encryption Protocol, Journal of Lightwave Technology, Vol.28 No.18, 2010.09.15, p.2714-2723, II. PRINCIPLE OF THE Y-00 ENCRYPTION PROTOCOL	1-5
A	JP 2007-193137 A (Fujitsu Ten Ltd.), 02 August 2007 (02.08.2007), paragraphs [0027] to [0051]	1-5
A	JP 2005-57313 A (Matsushita Electric Industrial Co., Ltd.), 03 March 2005 (03.03.2005), paragraphs [0043] to [0074]	1-5

☒ 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 March, 2011 (17.03.11)	29 March, 2011 (29.03.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/054688

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 2002-77135 A (NTT Fanet Systems Corp.), 15 March 2002 (15.03.2002), paragraphs [0017] to [0035]	1-5
A	JP 2002-40939 A (Yozan, Inc.), 08 February 2002 (08.02.2002), paragraphs [0017] to [0025]	1-5
A	JP 9-18473 A (Mitsubishi Electric Corp.), 17 January 1997 (17.01.1997), paragraphs [0031] to [0042]	1-5

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2011/054688

JP 2002-40939 A	2002.02.08	US 2002/0159481 A1

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０５４６８８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/20(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.　H04L9/20

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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）

JSTPlus/JMEDPlus/JST7580(JDreamII) Y-00

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	Ohhata, K. et al., 10-Gb/s Optical Transceiver Using the Yuen 2000 Encryption Protocol, Journal of Lightwave Technology, Vol.28 No.18, 2010.09.15, p.2714-2723, II. PRINCIPLE OF THE Y-00 ENCRYPTION PROTOCOL	1-5
A	JP 2007-193137 A（富士通テン株式会社）2007.08.02, 27-51段落	1-5
A	JP 2005-57313 A（松下電器産業株式会社）2005.03.03, 43-74段落	1-5

☑　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 １７．０３．２０１１	国際調査報告の発送日 ２９．０３．２０１１
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　９３６４ 中里　裕正 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 2002-77135 A（エヌ・ティ・ティ・ファネット・システムズ株式会社）2002.03.15, 17-35段落	1-5
A	JP 2002-40939 A（株式会社鷹山）2002.02.08, 17-25段落	1-5
A	JP 9-18473 A（三菱電機株式会社）1997.01.17, 31-42段落	1-5

国際調査報告
パテントファミリーに関する情報

国際出願番号 ＰＣＴ／ＪＰ２０１１／０５４６８８

JP 2002-40939 A	2002.02.08	US 2002/0159481 A1