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

特許第4906732号
(P4906732)

(45)発行日　平成24年3月28日(2012.3.28)　(24)登録日　平成24年1月20日(2012.1.20)

(51)Int.Cl.　　F I
H04K 1/00 (2006.01)　　H04K 1/00 Z
H04L 9/20 (2006.01)　　H04L 9/00 653

請求項の数 26　(全 23 頁)

(21)出願番号　特願2007-540948 (P2007-540948)
(86)(22)出願日　平成18年10月13日 (2006.10.13)
(86)国際出願番号　PCT/JP2006/320482
(87)国際公開番号　WO2007/046302
(87)国際公開日　平成19年4月26日 (2007.4.26)
審査請求日　平成21年8月31日 (2009.8.31)
(31)優先権主張番号　特願2005-302101 (P2005-302101)
(32)優先日　平成17年10月17日 (2005.10.17)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　110001276
特許業務法人　小笠原特許事務所
(72)発明者　佐田　友和
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　布施　優
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　古澤　佐登志
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】データ送信装置、データ受信装置、及びデータ通信装置

(57)【特許請求の範囲】
【請求項１】
暗号通信を行うデータ送信装置であって、
予め定められた所定の鍵情報と情報データとを入力し、信号レベルが略乱数的に変化する多値信号を発生する多値符号化部と、
前記多値信号に基づいて、所定の変調形式の変調信号を生成する変調部とを備え、
前記多値符号化部は、
前記鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する多値符号発生部と、
所定の処理に従って、前記多値符号列と前記情報データとを合成し、前記多値符号列と前記情報データとの組み合わせに対応したレベルを有する多値信号を生成する多値処理部とを含み、
前記多値符号発生部は、
前記鍵情報に基づいて２値乱数列を生成する乱数列生成部と、
所定の符号化則に従って、前記２値乱数列から前記多値符号列を生成する多値変換部とを有し、
前記所定の符号化則は、所定長の２値ビット系列を前記多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則であることを特徴とする、データ送信装置。

【請求項２】
前記多値符号発生部は、前記乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有することを特徴とする、請求項１に記載のデータ送信装置。
【請求項３】
前記ビットインターリーブのコラム数は、前記乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上であることを特徴とする、請求項２に記載のデータ送信装置。
【請求項４】
前記ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上であることを特徴とする、請求項２に記載のデータ送信装置。
【請求項５】
前記各多値レベルに対応付けられる２値ビット系列長が２以上であることを特徴とする、請求項１～４のいずれかに記載のデータ送信装置。
【請求項６】
前記多値レベルの総数が２のべき乗であることを特徴とする、請求項１～５のいずれかに記載のデータ送信装置。
【請求項７】
前記全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられることを特徴とする、請求項１～６のいずれかに記載のデータ送信装置。
【請求項８】
前記多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現されることを特徴とする、請求項１～７のいずれかに記載のデータ送信装置。
【請求項９】
暗号通信を行うデータ受信装置であって、
所定の変調形式の変調信号を復調し、多値信号を出力する復調部と、
予め定められた所定の鍵情報と前記多値信号とを入力し、情報データを出力する多値復号化部とを備え、
前記多値復号化部は、
前記鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する多値符号発生部と、
前記多値符号列に基づいて前記多値信号を識別し、前記情報データを出力する多値識別部とを含み、
前記多値符号発生部は、
前記鍵情報に基づいて２値乱数列を生成する乱数列生成部と、
所定の符号化則に従って、前記２値乱数列から前記多値符号列を生成する多値変換部とを有し、
前記所定の符号化則は、所定長の２値ビット系列を前記多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則であることを特徴とする、データ受信装置。
【請求項１０】
前記多値符号発生部は、前記多値符号発生部は、前記乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有することを特徴とする、請求項９に記載のデータ送信装置。
【請求項１１】
前記ビットインターリーブのコラム数は、前記乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上であることを特徴とする、請求項１０に記載のデータ受信装置。
【請求項１２】
前記ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上であることを特徴とする、請求項１０に記載のデータ受信装置。

【請求項１３】
前記各多値レベルに対応付けられる２値ビット系列長が２以上であることを特徴とする、請求項１０～１２のいずれかに記載のデータ受信装置。
【請求項１４】
前記多値レベルの総数が２のべき乗であることを特徴とする、請求項１０～１３のいずれかに記載のデータ受信装置。
【請求項１５】
前記全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられることを特徴とする、請求項１０～１４のいずれかに記載のデータ受信装置。
【請求項１６】
前記多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現されることを特徴とする、請求項１０～１５のいずれかに記載のデータ受信装置。
【請求項１７】
暗号通信を行うデータ通信装置であって、
前記データ通信装置は、データ送信装置と、データ受信装置とを備え、
前記データ送信装置は、
予め定められた所定の鍵情報と情報データとを入力し、信号レベルが略乱数的に変化する多値信号を発生する多値符号化部と、
前記多値信号に基づいて、所定の変調形式の変調信号を生成する変調部とを備え、
前記多値符号化部は、
前記鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する第１の多値符号発生部と、
所定の処理に従って、前記多値符号列と前記情報データとを合成し、前記多値符号列と前記情報データとの組み合わせに対応したレベルを有する多値信号を生成する多値処理部とを含み、
前記第１の多値符号発生部は、
前記鍵情報に基づいて２値乱数列を生成する第１の乱数列生成部と、
第１の符号化則に従って、前記２値乱数列から前記多値符号列を生成する第１の多値変換部とを有し、
前記第１の符号化則は、所定長の２値ビット系列を前記多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則であり、
前記データ受信装置は、
所定の変調形式の変調信号を復調し、多値信号を出力する復調部と、
予め定められた所定の鍵情報と前記多値信号とを入力し、情報データを出力する多値復号化部とを備え、
前記多値復号化部は、
前記鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する第２の多値符号発生部と、
前記多値符号列に基づいて前記多値信号を識別し、前記情報データを出力する多値識別部とを含み、
前記第２の多値符号発生部は、
前記鍵情報に基づいて２値乱数列を生成する第２の乱数列生成部と、
第２の符号化則に従って、前記２値乱数列から前記多値符号列を生成する第２の多値変換部とを有し、
前記第２の符号化則は、所定長の２値ビット系列を前記多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１

減じた値となるような規則であることを特徴とする、データ通信装置。
【請求項１８】
前記第１の多値符号発生部は、前記第１の乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有し、
前記第２の多値符号発生部は、前記第２の乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有することを特徴とする、請求項１７に記載のデータ通信装置。
【請求項１９】
暗号通信を行うための多値符号発生装置であって、
所定の鍵情報に基づいて２値乱数列を生成する乱数列生成部と、
所定の符号化則に従って、前記２値乱数列から前記多値符号列を生成する多値変換部とを有し、
前記所定の符号化則は、所定長の２値ビット系列を前記多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則であることを特徴とする、多値符号発生装置。
【請求項２０】
前記多値符号発生部は、前記乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有することを特徴とする、請求項１９に記載の多値符号発生装置。
【請求項２１】
前記ビットインターリーブのコラム数は、前記乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上であることを特徴とする、請求項２０に記載の多値符号発生装置。
【請求項２２】
前記ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上であることを特徴とする、請求項２０に記載の多値符号発生装置。
【請求項２３】
前記各多値レベルに対応付けられる２値ビット系列長が２以上であることを特徴とする、請求項１９～２２のいずれかに記載の多値符号発生装置。
【請求項２４】
前記多値レベルの総数が２のべき乗であることを特徴とする、請求項１９～２３のいずれかに記載の多値符号発生装置。
【請求項２５】
前記全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられることを特徴とする、請求項１９～２４のいずれかに記載の多値符号発生装置。
【請求項２６】
前記多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現されることを特徴とする、請求項１９～２５のいずれかに記載の多値符号発生装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、第３者による不法な盗聴・傍受を防ぐ暗号通信を行う装置に関する。より特定的には、正規の送受信者間で、特定の符号化／復号化（変調／復調）方式を選択・設定してデータ通信を行う装置に関する。
【背景技術】
【０００２】
従来、特定者同志でのみ通信を行うためには、送信／受信間で符号化／復号化のための元情報（鍵情報）を共有し、当該情報に基づいて、伝送すべき情報データ（平文）を数学的に演算／逆演算することにより秘密通信を実現する構成が採用されている。図２０は、

当該構成に基づく、従来のデータ送信装置の構成を示すブロック図である。図２０において、従来のデータ通信装置は、データ送信装置９００００１と、伝送路９１３と、データ受信装置９００００２とで構成される。データ送信装置９００００１は、符号化部９１１と、変調部９１２とからなる。データ受信装置９００００２は、復調部９１４と、復号化部９１５とからなる。ここで、符号化部９１１に情報データ９０と第１の鍵情報９１とを入力し、復号化部９１５に第２の鍵情報９６を入力すると、復号化部９１５から情報データ９８が出力される。さらに、第３者による盗聴行為を説明するため、図２０は、盗聴者復調部９１６と、盗聴者復号化部９１７とからなる盗聴者データ受信装置９００００３を含むものとする。盗聴者復号化部９１７には、第３の鍵情報９９が入力される。以下に、図２０を参照しながら、従来のデータ通信装置の動作を説明する。

【０００３】

データ送信装置９００００１において、符号化部９１１は、情報データ９０を、第１の鍵情報９１に基づいて符号化（暗号化）する。変調部９１２は、符号化部９１１で暗号化された情報データを所定の変調形式の変調信号９４に変換して伝送路９１３に送出する。データ受信装置９００００２において、復調部９１４は、伝送路９１３を介して伝送されてきた変調信号９４を所定の復調方式で復調し、暗号化された情報データを出力する。復号化部９１５は、符号化部９１１との間で共有した第１の鍵情報９１と同一の第２の鍵情報９６に基づいて、暗号化された情報データを復号化（暗号解読）して、元の情報データ９８を出力する。

【０００４】

盗聴者データ受信装置９００００３は、データ送信装置９００００１とデータ受信装置９００００２との間で伝送される変調信号（情報データ）を盗聴するに当たり、盗聴者復調部９１６が、伝送路９１３を伝搬する変調信号の一部を分岐、入力し、所定の復調方式で復調し、盗聴者復号化部９１７が第３の鍵情報９９に基づいて復号化を試みる。ここで、盗聴者復号化部９１７は、符号化部９１１との間で鍵情報を共有していないものとする。即ち、盗聴者復号化部９１７は、第１の鍵情報９１と異なる第３の鍵情報９９に基づき復号化を行うため、元の情報データを正しく再生することができない。

【０００５】

このような数学的な演算に基づく数理暗号（または、計算暗号、ソフトウェア暗号とも呼ばれる）技術は、例えば、特許文献１の公報にも記されているように、アクセスシステム等に適用できる。即ち、１つの光送信器から送出された光信号を光カプラで分岐し、複数の光加入者宅の光受信器にそれぞれ配信するＰＯＮ（Ｐａｓｓｉｖｅ　Ｏｐｔｉｃａｌ　Ｎｅｔｗｏｒｋ）構成では、各光受信器に、所望の光信号以外の他加入者に向けた信号が入力される。そこで、互いに異なる鍵情報を用いて、加入者毎の情報データを暗号化することによって、互いの情報の漏洩・盗聴を防ぎ、安全なデータ通信を実現することができる。

【特許文献１】特開平９－２０５４２０号公報

【非特許文献１】石橋啓一郎他訳、「暗号とネットワークセキュリティ：理論と実際」、ピアソン・エデュケーション、２００１年

【非特許文献２】安達真弓他訳、「暗号技術大全」、ソフトバンクパブリッシング、２００３年

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、数理暗号技術に基づく従来のデータ通信装置では、盗聴者は、たとえ鍵情報を共有しなくとも、暗号文（変調信号、または暗号化された情報データ）に対して、考え得る全ての組み合わせの鍵情報を用いた演算（総当たり攻撃）や、特殊な解析アルゴリズムの適用を試みれば、原理的に暗号解読が可能である。特に、近年の計算機の処理速度向上は目覚ましく、将来的に量子コンピュータ等の新しい原理による計算機が実現されれば、有限の時間内で、暗号文を盗聴できるという課題を有していた。

【０００７】
それ故に、本発明の目的は、盗聴者が暗号文の解析に要する時間を著しく増大させ、秘匿性の高いデータ通信装置を提供することである。
【課題を解決するための手段】
【０００８】
本発明は、暗号化通信を行うデータ送信装置に向けられている。そして上記目的を達成させるために、本発明のデータ送信装置は、予め定められた所定の鍵情報と情報データとを入力し、信号レベルが略乱数的に変化する多値信号を発生する多値符号化部と、多値信号に基づいて、所定の変調形式の変調信号を生成する変調部とを備える。多値符号化部は、鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する多値符号発生部と、所定の処理に従って、多値符号列と情報データとを合成し、多値符号列と情報データとの組み合わせに対応したレベルを有する多値信号を生成する多値処理部とを含む。多値符号発生部は、鍵情報に基づいて２値乱数列を生成する乱数列生成部と、所定の符号化則に従って、２値乱数列から多値符号列を生成する多値変換部とを有する。所定の符号化則は、所定長の２値ビット系列を多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則である。
【０００９】
好ましくは、多値符号発生部は、乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有する
【００１０】
好ましくは、ビットインターリーブのコラム数は、乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上である。また、ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上である。
【００１１】
好ましくは、各多値レベルに対応付けられる２値ビット系列長が２以上である。また、多値レベルの総数が２のべき乗である。また、全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられる。また、多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現される。
【００１２】
また、本発明は、暗号通信を行うデータ受信装置に向けられている。そして上記目的を達成させるために、本発明のデータ受信装置は、所定の変調形式の変調信号を復調し、多値信号を出力する復調部と、予め定められた所定の鍵情報と多値信号とを入力し、情報データを出力する多値復号化部とを備える。多値復号化部は、鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する多値符号発生部と、多値符号列に基づいて多値信号を識別し、情報データを出力する多値識別部とを含む。多値符号発生部は、鍵情報に基づいて２値乱数列を生成する乱数列生成部と、所定の符号化則に従って、２値乱数列から多値符号列を生成する多値変換部とを有する。所定の符号化則は、所定長の２値ビット系列を多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則である。
【００１３】
好ましくは、多値符号発生部は、多値符号発生部は、乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有する。
【００１４】
好ましくは、ビットインターリーブのコラム数は、乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上である。また、ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上である。
【００１５】

好ましくは、各多値レベルに対応付けられる２値ビット系列長が２以上である。また、多値レベルの総数が２のべき乗である。また、全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられる。また、多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現される。

【００１６】

また、本発明は、暗号通信を行うデータ通信装置にも向けられている。そして上記目的を達成させるために、本発明のデータ通信装置は、データ通信装置は、データ送信装置と、データ受信装置とを備える。データ送信装置は、予め定められた所定の鍵情報と情報データとを入力し、信号レベルが略乱数的に変化する多値信号を発生する多値符号化部と、多値信号に基づいて、所定の変調形式の変調信号を生成する変調部とを備える。多値符号化部は、鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する第１の多値符号発生部と、所定の処理に従って、多値符号列と情報データとを合成し、多値符号列と情報データとの組み合わせに対応したレベルを有する多値信号を生成する多値処理部とを含む。第１の多値符号発生部は、鍵情報に基づいて２値乱数列を生成する第１の乱数列生成部と、第１の符号化則に従って、２値乱数列から多値符号列を生成する第１の多値変換部とを有する。第１の符号化則は、所定長の２値ビット系列を多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則である。データ受信装置は、所定の変調形式の変調信号を復調し、多値信号を出力する復調部と、予め定められた所定の鍵情報と多値信号とを入力し、情報データを出力する多値復号化部とを備える。多値復号化部は、鍵情報から信号レベルが略乱数的に変化する多値符号列を発生する第２の多値符号発生部と、多値符号列に基づいて多値信号を識別し、情報データを出力する多値識別部とを含む。第２の多値符号発生部は、鍵情報に基づいて２値乱数列を生成する第２の乱数列生成部と、第２の符号化則に従って、２値乱数列から多値符号列を生成する第２の多値変換部とを有する。第２の符号化則は、所定長の２値ビット系列を多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則である。

【００１７】

好ましくは、第１の多値符号発生部は、第１の乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有する。第２の多値符号発生部は、第２の乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有する。

【００１８】

また、本発明は、暗号通信を行うための多値符号発生装置にも向けられている。そして上記目的を達成させるために、本発明の多値符号発生装置は、所定の鍵情報に基づいて２値乱数列を生成する乱数列生成部と、所定の符号化則に従って、２値乱数列から多値符号列を生成する多値変換部とを有する。所定の符号化則は、所定長の２値ビット系列を多値符号列の各多値レベルに一意に対応させ、かつ任意の隣接する多値レベルに割当てる２値ビット系列間の差異ビット数（ハミング距離）が、当該２値ビット系列長、あるいは当該２値ビット系列長より１減じた値となるような規則である

【００１９】

好ましくは、多値符号発生部は、乱数列生成部が生成した２値乱数列に対して、所定の深さのビットインターリブを行うインターリーブ部をさらに有する。

【００２０】

好ましくは、ビットインターリーブのコラム数は、乱数列生成部が生成した２値乱数列の線形複雑度の２倍以上である。また、ビットインターリーブの行数は、各多値レベルに対して割当てられる２値ビット系列長以上である。

【００２１】

好ましくは、各多値レベルに対応付けられる２値ビット系列長が２以上である。また、多値レベルの総数が２のべき乗である。また、全ての多値レベルに対して同じ系列長の２値ビット系列を割当てられる。また、多値レベルは、振幅、周波数、位相のいずれかの領域、もしくはいずれかの組み合わせで表現される。

【発明の効果】

【００２２】

本発明のデータ通信装置は、鍵情報に基づいて情報データを多値信号に符号化・変調し、受信した多値信号を同一の鍵情報に基づいて復調・符号化し、多値信号の信号対雑音電力比を適正化することにより、暗号文の解析に要する時間を著しく増大させ、秘匿性の高いデータ通信装置を提供することができる。

【００２３】

また、隣接多値レベルに割当てる２値ビット系列のハミング距離を増加させることにより、盗聴者が受信した２値乱数列に対して、より多くの誤りを誘発できる。このため、２値乱数列を生成するのに必要な初期値（すなわち鍵情報）を盗聴者が特定することが極めて困難となり、多値信号の多値数が比較的少ない場合でも高い秘匿性を確保することが可能となる。

【発明を実施するための最良の形態】

【００２４】

以下、本発明の実施形態について、図面を参照しながら説明する。

【００２５】

（第１の実施形態）

図１は、本発明の第１の実施形態に係るデータ通信装置の構成を示すブロック図である。図１において、データ通信装置は、多値符号化部１１１と、変調部１１２と、伝送路１１０と、復調部２１１と、多値復号化部２１２とで構成される。多値符号化部１１１は、第１の多値符号発生部１１１ａと、多値処理部１１１ｂとからなる。多値復号化部２１２は、第２の多値符号発生部２１２ａと、多値識別部２１２ｂとからなる。また、多値符号化部１１１と変調部１１２とでデータ送信装置１０１０１を構成し、復調部２１１と多値復号化部２１２とでデータ受信装置１０２０１を構成する。伝送路１１０には、ＬＡＮケーブルや同軸ケーブル等の金属路線や、光ファイバケーブル等の光導波路を用いることができる。また、伝送路１１０は、ＬＡＮケーブル等の有線ケーブルに限られず、無線信号を伝搬する自由な空間であってもよい。なお、図２および図３に、変調部１１２から出力される変調信号波形を説明するための模式図を示す。以下に、第１の実施形態について、図２および図３を用いながら、その動作を説明する。

【００２６】

第１の多値符号発生部１１１ａは、予め定められた所定の第１の鍵情報１１に基づいて、信号レベルが略乱数的に変化する多値符号列１２（図２（ｂ））を発生する。多値処理部１１１ｂは、多値符号列１２と情報データ１０（図２（ａ））とを入力し、所定の手順に従って両信号を合成し、当該信号レベルの組み合わせに対応したレベルを有する多値信号１３（図２（ｃ））を生成し、出力する。例えば、図２では、多値符号列１２がタイムスロットｔ１／ｔ２／ｔ３／ｔ４に対して当該レベルがｃ１／ｃ５／ｃ３／ｃ４と変化し、これをバイアスレベルとして、情報データ１０を加算することで、Ｌ１／Ｌ８／Ｌ６／Ｌ４と変化する多値信号１３を生成する。ここで、図３に示すように、情報データ１０の振幅を“情報振幅”、多値信号１３の全振幅を“多値信号振幅”、各バイアスレベル（多値符号列１２のレベル）ｃ１／ｃ２／ｃ３／ｃ４／ｃ５に対応して、多値信号１３が取り得るレベルの組（Ｌ１、Ｌ４）／（Ｌ２、Ｌ５）／（Ｌ３、Ｌ６）／（Ｌ４、Ｌ７）／（Ｌ５、Ｌ８）を、第１～第５の“基底”、多値信号１３の最小信号点間距離を“ステップ幅”とそれぞれ呼称する。変調部１１２は、多値信号１３を元データとして、所定の変調形式の変調信号１４に変換して、伝送路１１０に送出する。

【００２７】

復調部２１１は、伝送路１１０を介して伝送されてきた変調信号１４を復調し、上述し

た多値信号１５を再生する。第２の多値符号発生部２１２ａは、第１の鍵情報１１と同一の第２の鍵情報１６を予め共有し、当該第２の鍵情報１６に基づいて、多値符号列１２に相当する多値符号列１７を発生する。多値識別部２１２ｂは、多値符号列１７を閾値として、多値信号１５の識別（２値判定）を行い、情報データ１８を再生する。ここで、変調部１１２と復調部２１１とが、伝送路１１０を介して送受信する所定の変調形式の変調信号１４は、電磁波（電磁界）または光波を多値信号１３で変調して得られるものである。

【００２８】

なお、多値処理部１１１ｂにおける多値信号１３の生成については、上述のように、多値符号列１２と情報データ１０の加算処理による方法以外に、情報データ１０に従って、多値符号列１２のレベルを振幅変調／制御する方法や、あるいは、両信号レベルの組み合わせに対応した多値信号レベルを予め記憶させたメモリから、両信号レベルに応じて逐次読み出す方法等、いかなる手順であっても構わない。

【００２９】

図２および図３では、多値信号の多値数を“８”として表記したが、これに限定されるものではなく、それより大きくても小さくても良い。また、情報振幅を多値信号のステップ幅の３倍、もしくは整数倍として表記したが、いかなる奇数倍や偶数倍であっても良い。また、情報振幅は多値信号のステップ幅の整数倍でなくても構わない。さらに、これに関連して、図２および図３では、多値符号列の各レベル（各バイアスレベル）が、多値信号の各レベル間の略中心になるよう配置したが、これに限定されるものではなく、多値符号列の各レベルは、多値信号の各レベル間の略中心でなくても良いし、あるいは多値信号の各レベルに一致しても構わない。また、多値符号列と情報データとの変化レートが互いに等しく同期関係にあることを前提としたが、この限りではなく、一方の変化レートが他方より高速（または低速）であっても良いし、非同期であっても構わない。

【００３０】

次に、第３者による、変調信号の盗聴動作について説明する。当該第３者は、正規の受信者が備えるデータ受信装置１０２０１に準じた構成、もしくはさらに高性能なデータ受信装置（例えば、盗聴者データ受信装置）を用いて、変調信号を受信、解読することが想定される。盗聴者データ受信装置において、復調部（盗聴者復調部）は、変調信号を復調することにより、多値信号を再生する。しかし、多値復号化部（盗聴者多値復号化部）は、データ送信装置１０１０１との間で第１の鍵情報１１を共有しないため、データ受信装置１０２０１のように、当該鍵情報から発生した多値符号列を基準とした多値信号の２値判定を行うことができない。このような場合に考え得る盗聴動作としては、多値信号の全レベルに対する識別を同時に行う方法（一般に「総当たり攻撃」と呼ばれる）がある。即ち、盗聴者は、多値信号が取り得る全ての信号点間に対する閾値を用意して同時判定を行い、当該判定結果を解析することにより、正しい鍵情報または情報データを抽出する。例えば、盗聴者は、図２に示した多値符号列のレベルｃ０／ｃ１／ｃ２／ｃ３／ｃ４／ｃ５／ｃ６を閾値として用いて、多値信号に対する多値判定を行うことにより、当該レベルを同定する。

【００３１】

しかしながら、実際の伝送系では、種々の要因により雑音が発生し、これが変調信号に重畳されることによって、多値信号のレベルは、図４に示すように時間的・瞬時的に変動する。このような場合、正規受信者（データ受信装置１０２０１）による２値判定動作における被判定信号のＳＮ比（信号対雑音強度比）が、多値信号中の情報振幅と雑音量の比で決まるのに対して、盗聴者データ受信装置による多値判定動作における被判定信号のＳＮ被は、多値信号のステップ幅と雑音量との比によって決まる。このため、被判定信号が有する雑音レベルが同一条件下においては、盗聴者データ受信装置における被判定信号のＳＮ比が相対的に小さくなり、伝送特性（誤り率）が劣化することになる。即ち、第３者の全閾値による総当たり攻撃に対して識別誤りを誘発させて、盗聴を困難にすることができる。特に、多値信号のステップ幅を、当該雑音振幅（雑音強度分布の拡がり）に対して同オーダ、もしくは、より小さく設定すれば、第３者による多値判定を事実上不可能にし

て、理想的な盗聴防止を実現できる。

【００３２】

なお、上述のように被判定信号（多値信号、または変調信号）に重畳される雑音としては、変調信号に無線信号等の電磁波を用いた場合は、空間場や電子部品等が有する熱雑音（ガウス性雑音）を、光波を用いた場合は、熱雑音に加えて、光子が発生する際の光子数ゆらぎ（量子雑音）を、それぞれ利用できる。特に、量子雑音を伴った信号には、その記録や複製等の信号処理が適用できないことから、当該雑音量を基準に多値信号のステップ幅を設定することによって、第３者による盗聴を不可能として、データ通信の安全性を確保することができる。

【００３３】

以上説明したように、本実施形態によれば、伝送すべき情報データを多値信号として符号化し、当該信号点間距離を、当該雑音量に対して適切に設定することにより、第３者による盗聴時の受信信号品質に対して決定的な劣化を与えて、その解読・復号化を困難にする、安全なデータ通信装置を提供することができる。

【００３４】

（第２の実施形態）

図５は、本発明の第２の実施形態に係るデータ通信装置の構成を示すブロック図である。本図において、データ通信装置は、多値符号化部１１１と、変調部１１２と、伝送路１１０と、復調部２１１と、多値復号化部２１２と、第１のデータ反転部１１３と、第２のデータ反転部２１３とから構成され、図１の構成に対して、第１のデータ反転部１１３と、第２のデータ反転部２１３を新たに備える点が異なっている。また、多値符号化部１１１と、変調部１１２と、第１のデータ反転部１１３とで、データ送信装置１０１０２を構成し、復調部２１１と、多値復号化部２１２と、第２のデータ反転部２１３とで、データ受信装置１０２０２を構成する。以下に、本実施形態の動作を説明する。

【００３５】

本実施形態の構成は、前述の第１の実施形態（図１）に準ずるため、同一の動作を行うブロックに関しては、同一の参照符号を付して、その説明を省略し、相違点のみを説明する。その構成において、第１のデータ反転部１１３は、情報データが有する“０”と“１”の情報と、ＬｏｗレベルとＨｉｇｈレベルとの対応関係を固定せず、所定の手順で当該対応関係を略ランダムに変更する。例えば、多値符号化部１１１と同様、所定の初期値に基づいて発生させた乱数系列（疑似乱数列）との排他的論理和ＸＯＲ（Ｅｘｃｌｕｓｉｖｅ　ＯＲ）演算を行い、その演算結果を多値符号化部１１１に出力する。第２のデータ反転部２１３は、第１のデータ反転部１１３と逆の手順で、多値復号化部２１２から出力されたデータが有する“０”と“１”の情報と、ＬｏｗレベルとＨｉｇｈレベルとの対応関係を変更する。例えば、第２のデータ反転部２１３は、第１のデータ反転部１１３が備える初期値と同一の初期値を共有し、これに基づいて発生させた乱数のビット反転系列と多値符号化部２１２から出力されたデータとの排他的論理和演算を行い、その結果を情報データとして出力する。

【００３６】

以上説明したように、本実施形態によれば、伝送すべき情報データの反転を略ランダムに行うことにより、暗号としての多値信号の複雑性を大きくして、第３者による解読・復号化をさらに困難とし、より安全なデータ通信装置を提供することができる。

【００３７】

（第３の実施形態）

図６は、本発明の第３の実施形態に係るデータ通信装置の構成を示すブロック図である。図６において、データ通信装置は、多値符号化部１１１と、変調部１１２と、伝送路１１０と、復調部２１１と、多値復号化部２１２と、雑音制御部１１４とから構成され、図１の構成に対して、雑音制御部１１４を新たに備える点が異なっている。さらに、雑音制御部１１４は、雑音発生部１１４ａと、合成部１１４ｂとからなる。また、多値符号化部１１１と、変調部１１２と、雑音制御部１１４とで、データ送信装置１０１０３を構成し

、復調部２１１と、多値復号化部２１２とで、データ受信装置１０２０１を構成する。以下に、本実施形態の動作を説明する。

【００３８】

本実施形態の構成は、前述の第１の実施形態（図１）に準ずるため、同一の動作を行うブロックに関しては、同一の参照符号を付して、その説明を省略し、相違点のみを説明する。雑音制御部１１４において、雑音発生部１１４ａは、所定の雑音を発生する。合成部１１４ｂは、所定の雑音と多値信号１３とを合成して、合成した信号を変調部１１２に出力する。即ち、雑音制御部１１４は、図４で説明した多値信号のレベル変動を故意に生じさせて、多値信号のＳＮ比を任意の値に制御し、これにより、多値識別部２１２ｂに入力する被判定信号のＳＮ比を制御する。なお、前述したように、雑音発生部１１４ａで発生する雑音としては、熱雑音や量子雑音等が利用される。また、雑音が合成（重畳）された多値信号を雑音重畳多値信号２２と呼ぶことにする。

【００３９】

以上説明したように、本実施形態によれば、伝送すべき情報データを多値信号として符号化し、そのＳＮ比を任意に制御することにより、第３者による盗聴時の受信信号品質に対して決定的な劣化を故意に与え、その解読・復号化をさらに困難にする、より安全なデータ通信装置を提供することができる。

【００４０】

（第４の実施形態）

本発明の第４の実施形態に係るデータ通信装置の動作を説明する。本実施形態の構成は、前述の第１の実施形態（図１）、または第３の実施形態（図６）に準ずるため、構成図は省略する。第４の実施形態において、多値符号化部１１１は、図７に示すように、多値信号の各ステップ幅（Ｓ１～Ｓ７）を、各レベルの変動量、即ち各レベルに重畳されている雑音強度分布に従い設定する。具体的には、多値識別部２１２ｂに入力する被判定信号の隣り合う２つの信号点間で決まるＳＮ比が略一致するように、当該信号点間距離を配分する。なお、各レベルに重畳される雑音量が等しい場合には、各ステップ幅を均等に設定する。

【００４１】

一般に、変調部１１２から出力される変調信号として、半導体レーザ（ＬＤ）を光源とする光強度変調信号を想定した場合、ＬＤに入力する多値信号のレベルに依存して当該変動幅（雑音量）は変化する。これは、半導体レーザが自然放出光を「種光」とした誘導放出の原理に基づいて発光することに起因しており、その雑音量は、誘導放出光量に対する自然放出光量の相対比で定義されている。励起率（ＬＤに注入するバイアス電流に対応）が高い程、誘導放出光量の割合が大きくなるため、その雑音量は小さく、逆に、励起率が低い程、自然放出光量の割合が大きく、雑音量は大きくなる。そこで、図７に示すように、多値信号のレベルが小さい領域ではステップ幅を大きく、レベルが大きい領域では小さく、非線形に設定することにより、被判定信号の隣り合う信号点間のＳＮ比を一致させる。

【００４２】

また、変調信号として光変調信号を利用した場合でも、上記の自然放出光による雑音や光受信器に用いる熱雑音が充分小さい条件下では、受信信号のＳＮ比は、主にショット雑音で決定される。当該条件下では、多値信号のレベルが大きい程、当該雑音量が大きくなるため、図７の場合とは逆に、多値信号のレベルが小さい領域ではステップ幅を小さく、レベルが大きい領域では大きく設定することにより、被判定信号の隣り合う信号点間のＳＮ比を一致させる。

【００４３】

以上説明したように、本実施形態によれば、伝送すべき情報データを多値信号として符号化し、当該多値信号の信号点間距離を略均一に配置し、あるいは、瞬時レベルに依らず隣り合う信号点間のＳＮ比を略均一に設定することにより、第３者による盗聴時の受信信号品質を常に劣化させ、その解読・復号化をさらに困難にする、より安全なデータ通信装

置を提供することができる。

【００４４】

（第５の実施形態）

図８は、本発明の第５の実施形態に係るデータ通信装置の構成を示すブロック図である。図８において、データ通信装置は、データ送信装置１０１０５とデータ受信装置１０２０５とが伝送路１１０によって接続された構成である。データ送信装置１０１０５は、第１の多値符号発生部１５６ａのみが第１の実施形態と異なる。また、データ受信装置１０２０５は、第２の多値符号発生部２５６ａのみが第１の実施形態と異なる。

【００４５】

図９は、第１の多値符号発生部１５６ａの構成を示すブロック図である。図９において、第１の多値符号発生部１５６ａは、乱数列生成部１５７と、第１の多値変換部１５８とを有する。乱数列生成部１５７は、第１の鍵情報１１から２値乱数列を生成する。多値変換部１５８は、２値乱数列を多値符号列１２に変換する。なお、第２の多値符号発生部２５６ａの構成も第１の多値符号発生部１５６ａと同じである。

【００４６】

ここで、盗聴者による２値乱数列生成方法を特定する手法の１つとして、Ｂｅｒｌｅｋａｍｐ－Ｍａｓｓｅｙ法（以下ＢＭ法と略す）と呼ばれるアルゴリズムが存在する。これは、２ｋビット（ｋは２値乱数列の線形複雑度）の誤りのない２値乱数列から、当該２値乱数列の生成方法を特定するものである。従って、ＢＭ法による２値乱数列の生成方法の特定を防ぐためには、盗聴者が解読プロセスで得る２値乱数列中に、離散的な数多くの誤りを発生させることが望ましい。このような誤りの発生を実現する符号化方式として、まずは、誤りの個数を増加させる多値符号化方式について説明する。

【００４７】

図１０は、多値変換部１５８が２値乱数列を８値の多値符号列１２に変換するためのマッピング（割当）方法の一例を示す図である。図１０（ａ）は、２進数を１０進数に変換する方式（以下では２進－１０進符号化方式と表記）において、３ビットの２値ビット系列と多値レベルとの対応を示している。多値変換部１５８は、例えば、２値ビット系列“０００”、“００１”、“０１０”、・・・を、それぞれ“０”、“１”、“２”、・・・の多値レベルに変換する。

【００４８】

ここで、多値レベルに付加される干渉成分（ガウス雑音など）の確率密度分布は、図１０に示すように、送信者が送信した多値レベルをピークとした分布形状となることが多い。また、盗聴者が受信した多値レベルから発生する多値識別誤りは、隣接多値レベルへの識別誤りとなる確率が最も高くなる。この場合、盗聴者が多値符号列１２から得る２値乱数列に対して誘発可能な誤りの個数は、隣接多値レベルに割当てられた２値ビット系列のハミング距離（すなわち、差異ビット数）（以下では、隣接多値レベル間ハミング距離と表記）でほぼ決定される。しかし、２進－１０進符号化方式では、隣接多値レベル間ハミング距離が１（最小値）となる場合が多く、隣接多値識別誤りによって、２値乱数列に多くの誤りを誘発することは期待できない。

【００４９】

上記課題を鑑みて、隣接多値レベル間ハミング距離を最大化する方式（以下ではＭａｘｉｍｉｚｅｄ　Ｈａｍｍｉｎｇ　ｄｉｓｔａｎｃｅ（ＭＨ）符号化方式と表記）により、誤りの誘発効果を高める。図１０（ｂ）に示したＭＨ符号化方式では、例えば、多値レベル“０”、“１”、“２”、・・・に対して、２値ビット系列“０００”、“１１１”、“０１０”、・・・を対応させる。この方法により、隣接多値レベル間ハミング距離は、各多値レベルに割当てられた２値ビット系列長“３”と同等か、それよりも１小さい値“２”となり、平均的な隣接多値レベル間ハミング距離を増加することができる。このように、ＭＨ符号化方式を用いることで、盗聴者の２値乱数列により多くの誤りを誘発でき、解読に要する計算量を増加させることが可能となる。

【００５０】

続いて、ＭＨ符号化方式での多値符号列１２の生成アルゴリズムについて、図１０（ｂ）に示した８値の多値レベルマッピングを例に説明する。なお、ここに示す方法はあくまで一例であり、隣接多値レベル間ハミング距離を増加させる方法であれば、いかなる方法であっても構わない。また、以下では、多値レベル“０”、“１”、“２”、・・・、“ｉ”、・・・に割当てる２値ビット系列を、A_0、A_1、A_2、・・・、A_i、・・・と表す。

【００５１】

まず始めに、多値レベル“０”に割当てる２値ビット系列A_0を決定する。ここで割当てる２値ビット系列は任意であるが、一例としてA_0＝“０００”とする。次に、多値レベル“１”について、A_1はA_0（＝“０００”）を全て反転した“１１１”とし、A_1－A_0間のハミング距離として、３（最大値）を確保する。

【００５２】

続いて、多値レベル“２”について、A_2－A_1間のハミング距離を最大化するには、A_2＝“０００”とすることが望ましいが、この２値ビット系列はA_0と重複するため、別の割当て方法が必要である。そこで、A_2－A_1間のハミング距離が、２値ビット系列長よりも１小さい値である２となるように、A_1のうち２ビットを反転させた系列をA_2に割当てる。ここでは一例として、A_1の１及び３ビット目を反転し、A_2＝“０１０”とする。

【００５３】

次に、多値レベル“３”について、A_3はA_2（＝“０１０”）を全て反転した“１０１”とし、A_3－A_2間のハミング距離として、３（最大値）を確保する。

【００５４】

続いて、多値レベル“４”について、A_4－A_3間のハミング距離を最大化するには、A_4＝“０１０”とすることが望ましいが、この２値ビット系列はA_2と重複するため、別の割当て方法が必要である。そこで、A_4－A_3間のハミング距離が、２値ビット系列長よりも１小さい値である２となるように、A_3のうち２ビットを反転させた系列をA_4に割当てる。ここで、A_3の１及び３ビット目を反転させた場合、A_0と重複するため、ここでは一例として、A_3の２及び３ビット目を反転し、A_4＝“１１０”とする。

【００５５】

次に、多値レベル“５”について、A_5はA_4（＝“１１０”）を全て反転した“００１”とし、A_5－A_4間のハミング距離として、３（最大値）を確保する。

【００５６】

続いて、多値レベル“６”について、A_6－A_5間のハミング距離を最大化するには、A_6＝“１１０”とすることが望ましいが、この２値ビット系列はA_4と重複するため、別の割当て方法が必要である。そこで、A_6－A_5間のハミング距離が、２値ビット系列長よりも１小さい値である２となるように、A_5のうち２ビットを反転させた系列をA_6に割当てる。ここでは一例として、A_5の１及び３ビット目を反転し、A_6＝“１００”とする。

【００５７】

最後に、多値レベル“７”について、A_7はA_6（＝“１００”）を全て反転した“０１１”とし、A_7－A_6間のハミング距離として、３（最大値）を確保する。

【００５８】

上記の方法により、全ての多値レベルに対して一意に対応し、かつ隣接多値レベル間ハミング距離が２値ビット系列長“３”、あるいはそれより１減じた２値ビット系列長“２”となる２値ビット系列を割当てることができる。

【００５９】

また、上記の例で示したように、各多値レベルに割り当てられる２値ビット系列長がすべて同じであり、多値数が２のべき乗である場合には、多値レベルと２値ビット系列とのマッピング方法を、計算により求めることも可能である。下記では、この計算方法を説明するにあたって、まずは、反転ビット行列及び反転ビット系列を定義する。

【００６０】

（式１）には、反転ビット行列C_i（ｉは自然数）を定義する漸化式を示す。（式１）

に示すように、反転ビット行列C_iは、それぞれ列数“ｉ”、行数“2^i-1”の行列であり、このような漸化式に従って生成される。ここで、漸化式の初期値C_1を１とし、求めるべき反転ビット行列の多値数をＭとした場合、反転ビット行列はC_{log2M}となる。（式２）には、ｉ＝１，２，３の場合の反転ビット行列Ｃｉの一例を示す。例えば、（式２）に示すように、多値数が８（Ｍ＝８）の場合には、上述した漸化式に従ってC_3が算出される。ここで算出されたC_3の各行の要素B_0、B_1、・・・、B_6を反転ビット系列として定義する。

【数１】

$$C_{n+1}=\left[\begin{array}{c|c} 1 & \\ \vdots & C_n \\ 1 & \\ \hline 0 & 11\cdots1 \\ \hline 1 & \\ \vdots & C_n \\ 1 & \end{array}\right] \qquad \cdots\ (式1)$$

【数２】

$$C_1=[1]$$

$$C_2=\left[\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \\ \hline 1 & 1 \end{array}\right] \qquad \cdots\ (式2)$$

$$C_3=\left[\begin{array}{c|cc} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ \hline 0 & 1 & 1 \\ \hline 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{array}\right]=\left[\begin{array}{c} B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{array}\right]$$

【００６１】

続いて、図１１には、ＭＨ符号化方式において、各多値レベルに割り当てる２値ビット系列と反転ビット系列との対応関係を示す。ここで、ＥＸＯＲ（Ａ，Ｂ）を、２値ビット系列Ａ及びＢの排他的論理和演算と表現とした場合、図１１に示すように、８値の多値レベルに対してそれぞれ割り当てられる２値ビット系列A_0～A_7は、（式３）に示す関係で定義される。ここで、A_0は初期値として、任意の２値ビット系列を割り当てることが可能であるが、例えばA_0＝“０００”とすれば、図１０（ｂ）に示したＭＨ符号化方式の２値ビット系列と同等のマッピング方法を導出することが可能となる。

【数３】

$$A_{i+2}=EXOR(A_i,B_i) \qquad \cdots\ (式3)$$

【００６２】

上記に示した方法により、盗聴者の多値識別誤りが、２値乱数列に対して誘発する誤りの個数を増加させることが可能となり、２値乱数列の特定を困難化することができる。

【００６３】

なお、上述したＭＨ符号化に従った多値符号列１２の生成は、一例として、予めメモリなどに記憶された２値乱数列と多値符号列１２との対応関係に基づいて、２値乱数列から多値符号列１２を生成する方法が考えられる。また、その他の例として、多値変換部１５８は、以下に示す構成に従って、多値符号列１２を生成することもできる。

【００６４】

図１２は、多値変換部１５８の詳細な構成の一例を示すブロック図である。図１２を参照して、多値変換部１５８は、シリアル－パラレル変換部１５８１と、符号変換部１５８２と、Ｄ／Ａ変換部１５８３とから構成される。シリアル－パラレル変換部１５８１は、入力された２値乱数列をシリアル－パラレル変換して出力する。図１３は、シリアル－パラレル変換部１５８１の具体的な構成の一例を示す図である。シリアル－パラレル変換部１５８１は、例えば図１３に示すように、シリアルポートに入力された２値乱数列を、パラレルポートのＬＳＢ側からＭＳＢ側に向けて１ビットずつ順に出力し、ＭＳＢに達した次のビットを再びＬＳＢ側から順に出力する。なお、パラレルポートのポート数ｍは$\log_2 M$（Ｍは多値符号列１２の多値数）とする。ここで、パラレルポートのＬＳＢ側から順に、パラレルポート番号＃１、＃２、・・・＃ｍとした場合、シリアルポートに入力されるｉ番目の２値乱数列は、パラレルポート番号＃（ｍｏｄ（ｉ－１，ｍ）＋１）から出力される。ただし、ｍｏｄ（ａ，ｂ）はａをｂで割ったときの余りである。

【００６５】

図１４は、符号変換部１５８２の構成の一例を示すブロック図である。符号変換部１５８２は、例えば図１４に示すように、入力ポート（ポート数：ｍ）に入力された２値乱数列を、ＥＸＯＲ素子によって変換し、出力ポート（ポート数：ｍ）から出力する。なお、図１４には、一例として多値数（Ｍ＝１６）の場合を示しており、入力ポート、出力ポートのポート数ｍは４となる。ここで、ＬＳＢ側からｉ番目の入力ポートに入力される符号をX_i、ＬＳＢ側からｊ番目の出力ポートに出力される符号をY_jとする。

【００６６】

このとき、入力X_1～X_4に対して、出力Y_1～Y_4が、$Y_1=X_1$、Y_2＝ＥＸＯＲ（X_1，X_2，X_3）、Y_3＝ＥＸＯＲ（X_1，X_3，X_4）、Y_4＝ＥＸＯＲ（X_1，X_4）となるように論理演算を行う。この論理演算を一般化すると、多値数が２（ポート数ｍ＝１）の場合は$Y_1=X_1$（変換なし）、多値数が４（ポート数＝２）の場合は$Y_1=X_1$、Y_2＝ＥＸＯＲ（X_1、X_2）、多値数が８以上の２のべき乗数（ポート数ｍ：３以上）の場合は、２≦ｉ≦（ｍ－１）を満たす整数ｉに対して、$Y_1=X_1$、Y_i＝ＥＸＯＲ（X_1，X_i，X_{i+1}）、Y_m＝ＥＸＯＲ（X_1，X_m）となる。

【００６７】

Ｄ／Ａ変換部１５８３は、符号変換された２値乱数列をＤ／Ａ変換し、多値符号列１２として出力する。例えば、Ｄ／Ａ変換部１５８３は、ｍ個の入力ポートと１つの出力ポートとを有しており、ＬＳＢ側からｉ番目のポートへの入力をそれぞれ2^{i-1}倍した後、これら全てを加算した結果を出力する。以上の構成により、多値変換部１５８は、ＥＸＯＲ素子を利用して、ＭＨ符号を生成することが可能となる。なお、ＭＨ符号の生成方法は上記に限るものではない。

【００６８】

また、多値変換部１５８は、（式４）に示すように、（2^n-1）行×ｎ列の反転ビット行列Ｃｎを、（2^n-1）行×ｋ列の行列Ｃｎ’と、（2^n-1）行×（ｎ－ｋ）列の行列Ｃｎ’’（ｋは１以上、（ｎ－１）以下の任意の整数）とに分け、（式５）に示す漸化式を用いて、反転ビット行例を算出してもよい。

【数４】

$$C_n = \underbrace{\left[\underbrace{C_n'}_{k\text{列}} \quad \underbrace{C_n''}_{(n-k)\text{列}} \right]}_{(2^n-1)\text{行}} \quad \cdots \text{（式４）}$$

【数５】

$$C_{n+1} = \begin{bmatrix} C_n' & \begin{matrix}1\\ \vdots \\ 1\end{matrix} & C_n'' \\ 1\cdots 1 & 0 & 1\cdots 1 \\ C_n' & \begin{matrix}1\\ \vdots \\ 1\end{matrix} & C_n'' \end{bmatrix} \quad \cdots \text{（式５）}$$

（k列　1列　$(n-k)$列）

【００６９】
以上のように、本実施形態によれば、隣接多値レベルに割当てる２値ビット系列のハミング距離を増加させることにより、盗聴者が受信した２値乱数列に対して、より多くの誤りを誘発できる。このため、２値乱数列を生成するのに必要な初期値（すなわち鍵情報）を盗聴者が特定することが極めて困難となり、多値信号の多値数が比較的少ない場合でも高い秘匿性を確保することが可能となる。

【００７０】
（第６の実施形態）
第５の実施形態において説明した方法により、盗聴者が得る２値乱数列に含まれる誤りの個数を増加させることが可能である。しかし、ＢＭ法などによる解読を防ぐためには、誤りの個数増加に加えて、さらに、誤りを離散化させることが望ましい。

【００７１】
本実施形態では、誤りを離散化させる方法について、第１の実施形態に示した構成を元に、差分を重点的に説明する。

【００７２】
図１５は、本発明の第６の実施形態に係るデータ通信装置の構成を示すブロック図である。図１５において、データ通信装置は、データ送信装置１０１０６とデータ受信装置１０２０６とが伝送路１１０によって接続された構成である。データ送信装置１０１０６は、第１の多値符号発生部１６６ａのみが第１の実施形態と異なる。データ受信装置１０２０６は、第２の多値符号発生部２６６ａのみが第１の実施形態と異なる。

【００７３】
図１６は、第１の多値符号発生部１６６ａの構成を示すブロック図である。図１６において、第１の多値符号発生部１６６ａは、乱数列生成部１６７と、インターリーブ部１６８と、多値変換部１６９とを有する。乱数列生成部１６７は、第１の鍵情報１１から第１の２値乱数列を生成する。インターリーブ部１６８は、第１の２値乱数列をビットインタリーブし、第２の２値乱数列として出力する。多値変換部１６９は、第２の２値乱数列を多値符号列１２に変換する。

【００７４】
この場合、盗聴者が、乱数列生成部１６７の乱数列生成方法を特定するためには、多値

信号１３を使用されている多値符号化方式に基づいて２値化し、第２の２値乱数列を得た上で、送信者及び正規受信者がインターリーブ部１６８で行うビットインターリーブとは逆の作業（逆インターリーブ）を行って、第１の２値乱数列を得ることが必要となる。

【００７５】

図１７には、盗聴者が受信した多値信号１３において、多値識別誤りが同じ位置に発生した場合に得られる２値乱数列の誤り分布（評価例）を示す。図１７（ａ）を参照して、２進－１０進符号化方式（インターリーブなし）の場合には、２値乱数列に含まれる誤りの個数が少なく、長周期の誤りフリー区間が数多く存在している。従って、ＢＭ法などにより即座に２値乱数列の生成方法を特定される可能性が高いと考えられる。続いて、図１７（ｂ）を参照して、ＭＨ符号化方式（インターリーブなし）の場合には、誤りの個数が増加しているが、誤りが局在化しており、依然として長周期の誤りフリー区間が多数存在している。従って、ＢＭ法などにより２値乱数列の生成方法を特定される可能性があると考えられる。図１７（ｃ）を参照して、ＭＨ符号化に、本実施例で示すインターリーブを併用した場合には、図１７（ｂ）で示すような局在化した誤りが離散化され、誤りフリー区間が大幅に減少している。従って、ＭＨ符号化とインターリーブの併用により、ＢＭ法などによる解読耐性を高めることが可能となる。

【００７６】

図１８は、インターリーブ行数と解読計算量との関係を示す図である。図１８のグラフは、２値乱数列の線形複雑度を１０、多値数を２５６、インターリーブ行数を１とした場合の所要受信ビット数を基準に、インターリーブ行数を変更した場合の所要受信ビット数の比率を解読計算量として示している。図１８に示すように、多値数が１６（＝2^4）の場合はインターリーブ行数が４以上、多値数が２５６（＝2^8）の場合はインターリーブ行数が８以上で、解読計算量は飽和する特性を有する。すなわち、インターリーブ部１６８は、インターリーブ行数を各多値レベルに割り当てる２値ビット系列長以上に設定すれば、解読計算量を最大化することが可能となる。

【００７７】

図１９は、インターリーブ列数と解読計算量の関係を示す図である。図１９に示すグラフは、２値乱数列の線形複雑度を５、多値数を２５６、インターリーブ列数を１とした場合の所要受信ビット数を基準に、インターリーブ列数を変更した場合の所要受信ビット数の比率を解読計算量として示している。図１９に示すように、線形複雑度が５の場合はインターリーブ列数が１０以上、線形複雑度が１０の場合はインターリーブ列数が２０以上で、解読計算量が飽和する特性を有する。すなわち、インターリーブ部１６８は、インターリーブ列数を線形複雑度の２倍以上に設定すれば、解読計算量を最大化することが可能となる。

【００７８】

なお、第５及び第６の実施形態は、第１～第４の実施形態に適用することができる。また、第１～６の実施形態に係るデータ通信装置は、データ通信を行うための方法としても捉えることができる。

【産業上の利用可能性】

【００７９】

本発明に係るデータ通信装置は、盗聴・傍受等に対して安全な秘密通信装置等として有用である。

【図面の簡単な説明】

【００８０】

【図１】本発明の第１の実施形態に係るデータ通信装置の構成を示すブロック図

【図２】本発明の第１の実施形態に係るデータ通信装置の伝送信号波形を説明する模式図

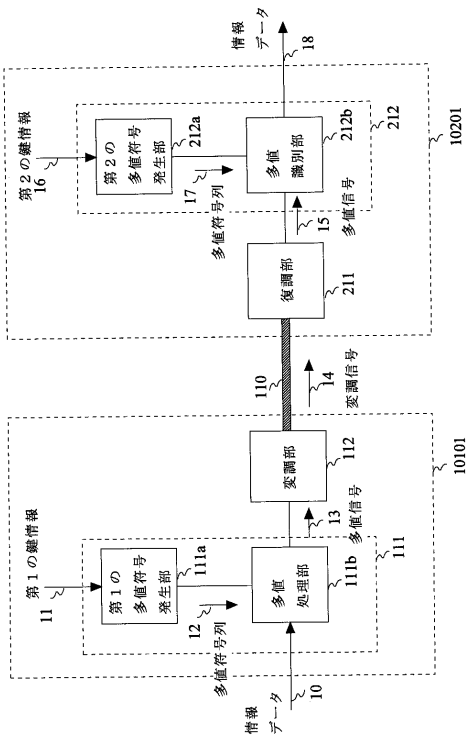
【図３】本発明の第１の実施形態に係るデータ通信装置の伝送信号波形の呼称を説明する模式図

【図４】本発明の第１の実施形態に係るデータ通信装置の伝送信号品質を説明する模式図

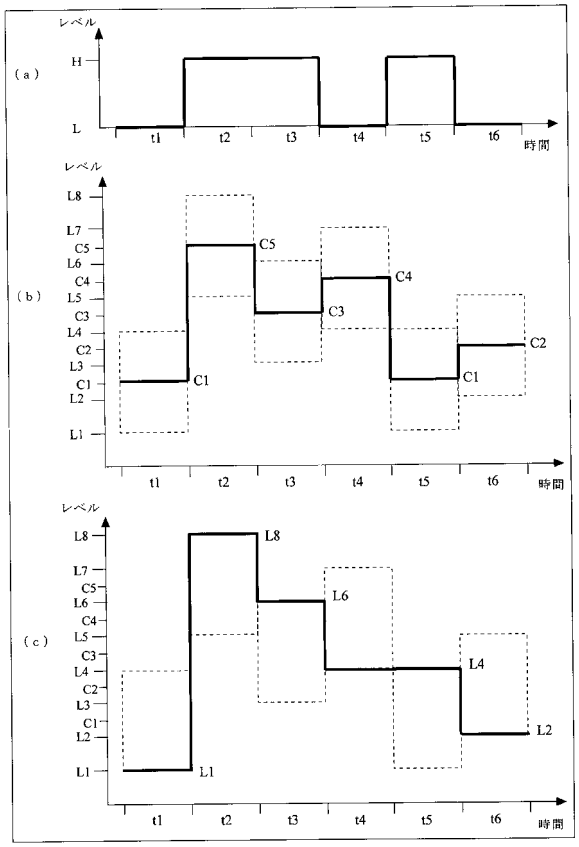
【図５】本発明の第２の実施形態に係るデータ通信装置の構成を示すブロック図

【図６】本発明の第３の実施形態に係るデータ通信装置の構成を示すブロック図
【図７】本発明の第４の実施形態に係るデータ通信装置の伝送信号パラメータを説明する模式図
【図８】本発明の第５の実施形態に係るデータ通信装置の構成を示すブロック図
【図９】第１の多値符号発生部１５６ａの構成を示すブロック図
【図１０】多値変換部１５８が２値乱数列を８値の多値符号列１２に変換するためのマッピング（割当）方法の一例を示す図
【図１１】ＭＨ符号化方式において、各多値レベルに割り当てる２値ビット系列と反転ビット系列との対応関係を示す図
【図１２】多値変換部１５８の詳細な構成の一例を示すブロック図
【図１３】シリアル－パラレル変換部１５８１の具体的な構成の一例を示す図
【図１４】符号変換部１５８２の構成の一例を示すブロック図
【図１５】本発明の第６の実施形態に係るデータ通信装置の構成を示すブロック図
【図１６】第１の多値符号発生部１６６ａの構成を示すブロック図
【図１７】多値識別誤りが同じ位置に発生した場合に得られる２値乱数列の誤り分布を示す図
【図１８】インターリーブ行数と解読計算量との関係を示す図
【図１９】インターリーブ列数と解読計算量の関係を示す図
【図２０】従来のデータ送信装置の構成を示すブロック図
【符号の説明】
【００８１】
１０１０１，１０１０２，１０１０３，１０１０５，１０１０６　データ送信装置
１１０　伝送路
１１１　多値符号化部
１１１ａ　第１の多値符号発生部
１１１ｂ　多値処理部
１１２　変調部
１１３　第１のデータ反転部
１１４　雑音制御部
１１４ａ　雑音発生部
１１４ｂ　合成部
１５６ａ，２５６ａ　多値符号発生部
１５７　乱数列生成部
１５８　多値変換部
１５８１　シリアル－パラレル変換部
１５８２　符号変換部
１５８３　Ｄ／Ａ変換部
１６６ａ、２６６ａ　多値符号発生部
１６７　乱数列生成部
１６８　インターリーブ部
１６９　多値変換部
１０２０１，１０２０２，１０２０５，１０２０６　データ受信装置
２１１　復調部
２１２　多値復号化部
２１２ａ　第２の多値符号発生部
２１２ｂ　多値識別部
２１３　第２のデータ反転部

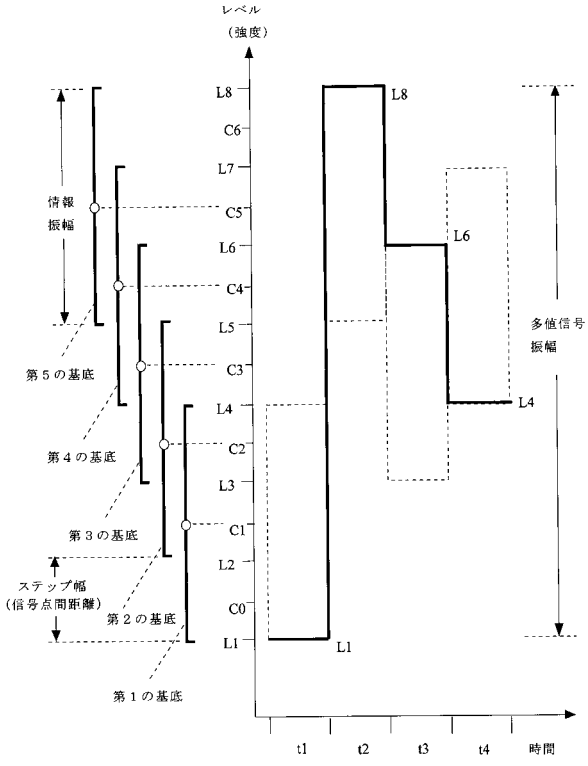
【図１】


情報データ
18
第２の鍵情報
16
第２の多値符号発生部
212a
多値識別部
212b
212
10201
17
多値符号列
15
多値信号
復調部
211
110
14
変調信号
変調部
112
10101
第１の鍵情報
11
第１の多値符号発生部
111a
多値処理部
111b
111
13
多値信号
12
多値符号列
10
情報データ

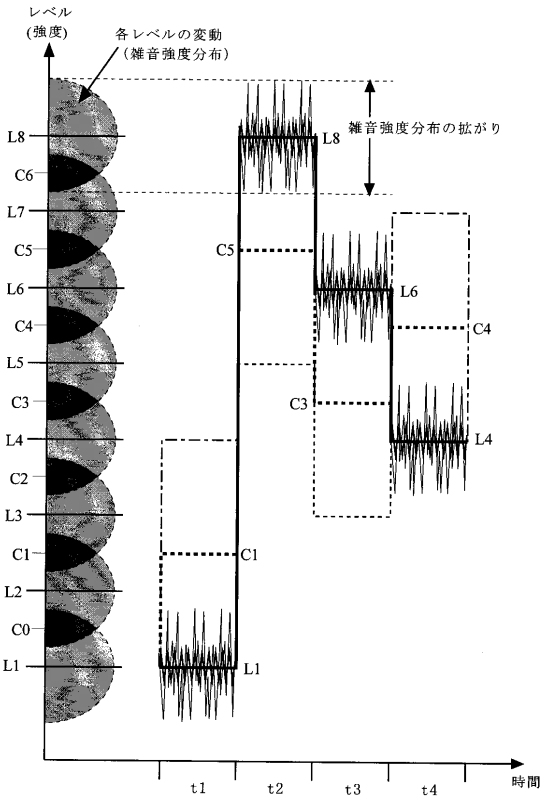
【図２】


(a)
レベル
H
L
t1 t2 t3 t4 t5 t6
時間
(b)
L8 L7 C5 L6 C4 L5 C3 L4 C2 L3 C1 L2 L1
C5 C4 C3 C2 C1 C1
(c)
L8 L7 C5 L6 C4 L5 C3 L4 C2 L3 C1 L2 L1
L8 L6 L4 L2 L1

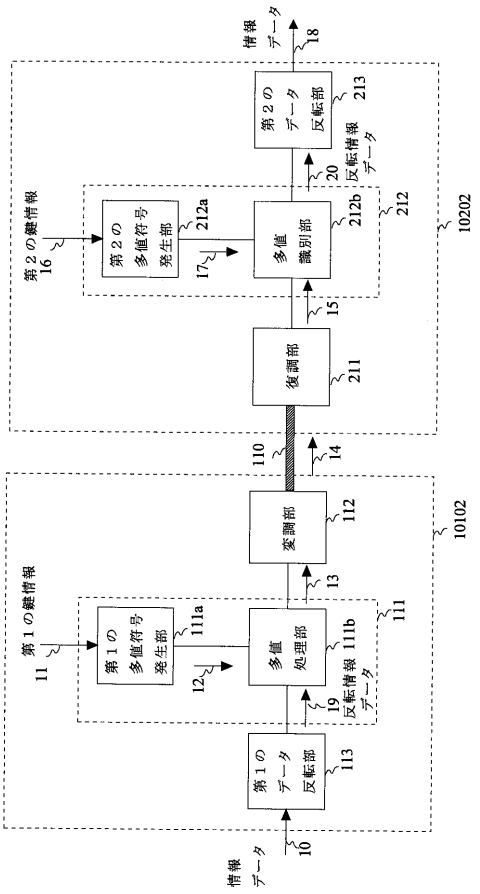
【図３】


レベル
(強度)
L8 C6 L7 C5 L6 C4 L5 C3 L4 C2 L3 C1 L2 C0 L1
情報振幅
第５の基底
第４の基底
第３の基底
ステップ幅
(信号点間距離)
第２の基底
第１の基底
多値信号振幅
t1 t2 t3 t4 時間

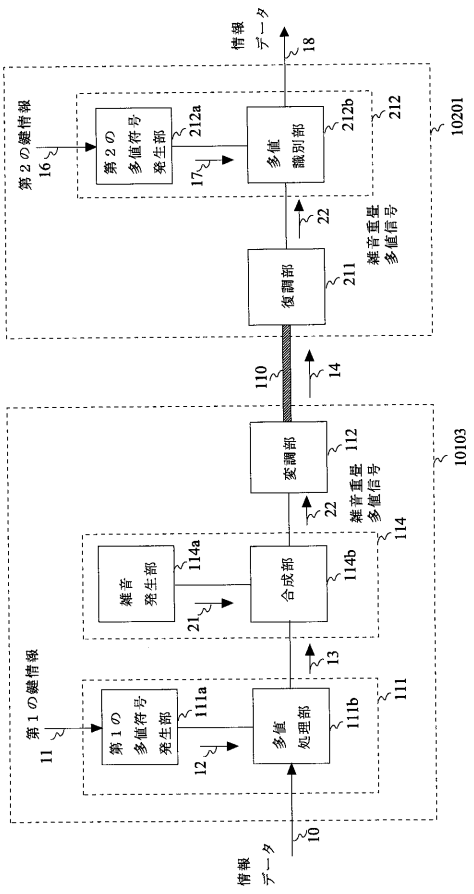
【図４】


レベル
(強度)
各レベルの変動
(雑音強度分布)
雑音強度分布の拡がり
L8 C6 L7 C5 L6 C4 L5 C3 L4 C2 L3 C1 L2 C0 L1
t1 t2 t3 t4 時間

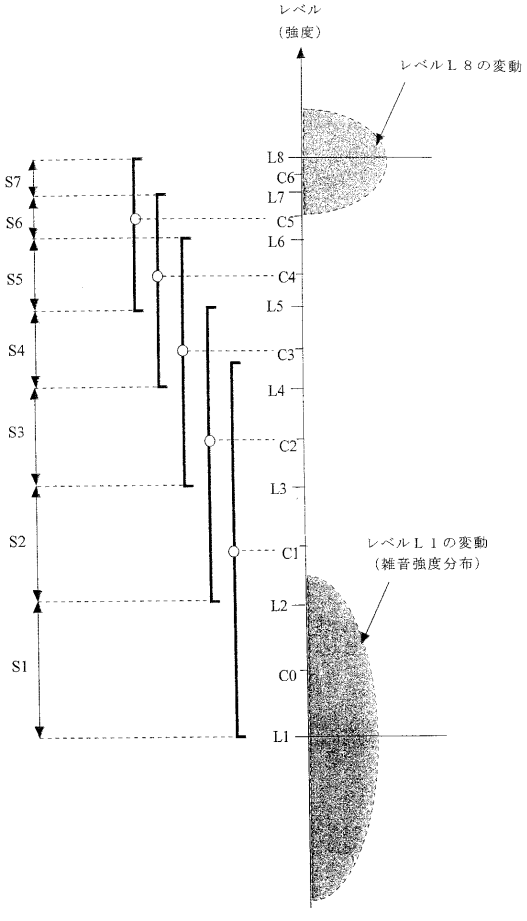
【図５】


情報データ
18
第２のデータ反転部
213
反転情報データ
20
第２の鍵情報
16
第２の多値符号発生部
212a
17
多値識別部
212b
212
10202
15
復調部
211
110
14
変調部
112
13
第１の鍵情報
11
第１の多値符号発生部
111a
12
多値処理部
111b
111
反転情報データ
19
第１のデータ反転部
113
10102
情報データ
10

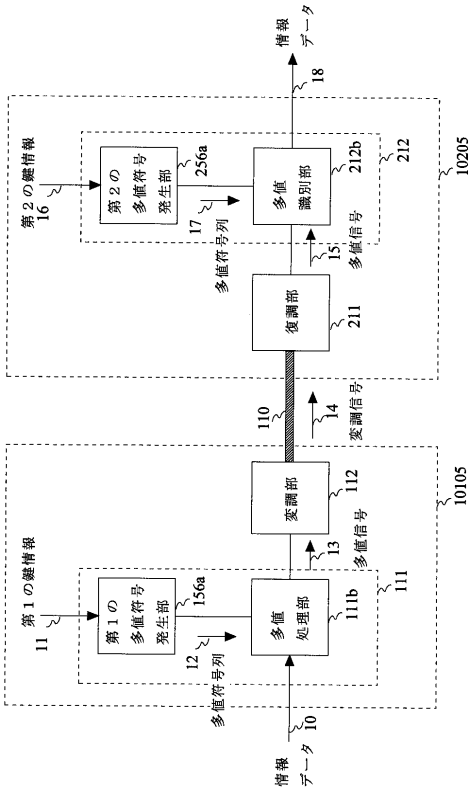
【図６】


情報データ
18
第２の鍵情報
16
第２の多値符号発生部
212a
17
多値識別部
212b
212
10201
22
雑音重畳多値信号
復調部
211
110
14
変調部
112
10103
雑音発生部
114a
21
合成部
114b
114
第１の鍵情報
11
第１の多値符号発生部
111a
12
多値処理部
111b
111
13
情報データ
10

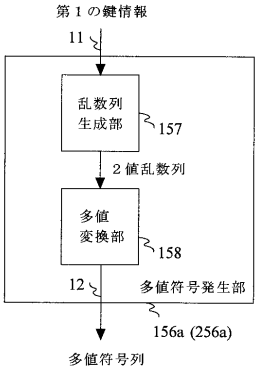
【図７】


レベル
（強度）
レベルＬ８の変動
L8
C6
L7
C5
L6
C4
L5
C3
L4
C2
L3
C1
L2
C0
L1
S7
S6
S5
S4
S3
S2
S1
レベルＬ１の変動
（雑音強度分布）

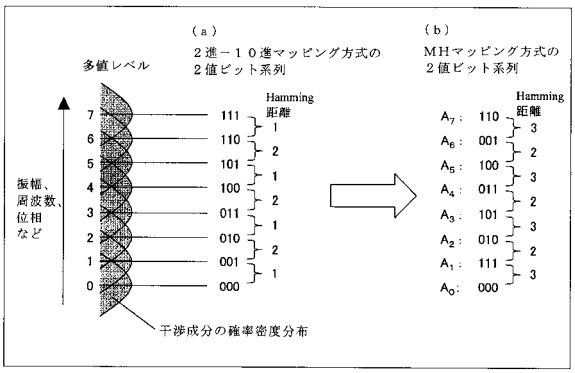
【図８】


情報データ
18
第２の鍵情報
16
第２の多値符号発生部
256a
17
多値識別部
212b
212
10205
多値符号列
15
多値信号
復調部
211
110
14
変調信号
変調部
112
10105
第１の鍵情報
11
第１の多値符号発生部
156a
12
多値処理部
111b
111
13
多値信号
多値符号列
10
情報データ

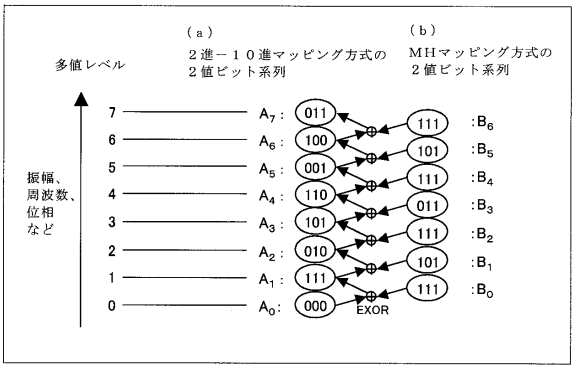
【図９】



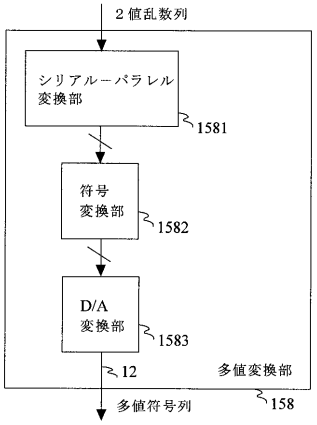
【図１０】



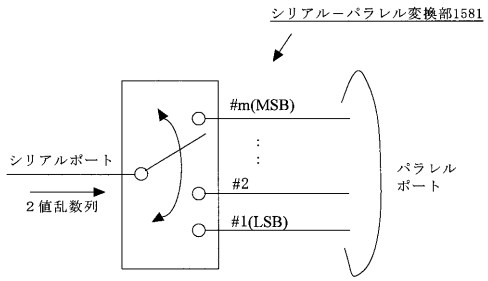
【図１１】



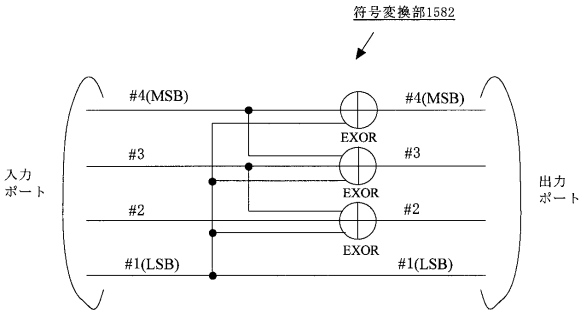
【図１２】



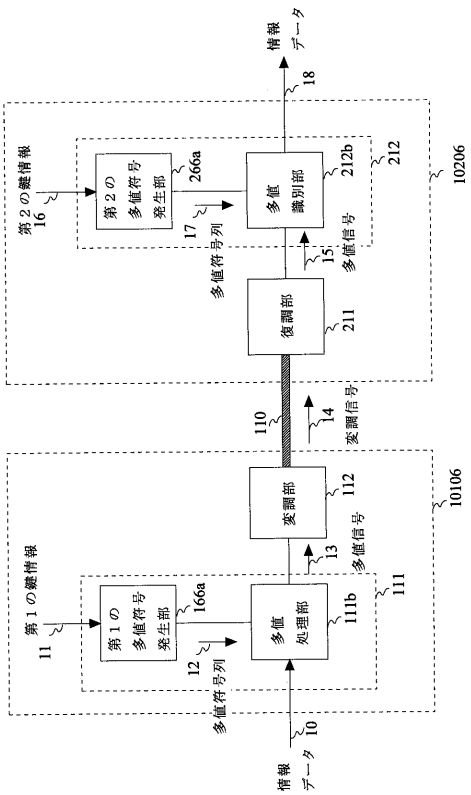
【図１３】



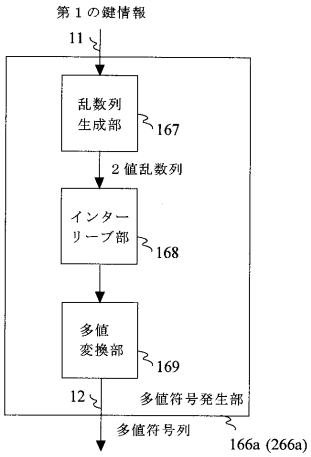
【図１４】



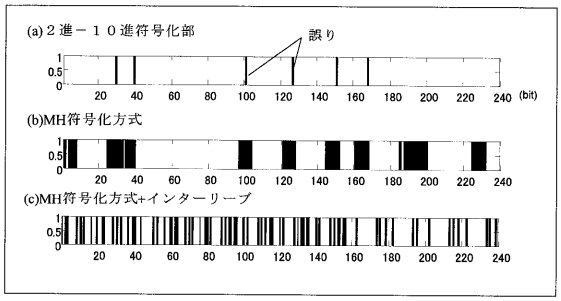
【図１５】



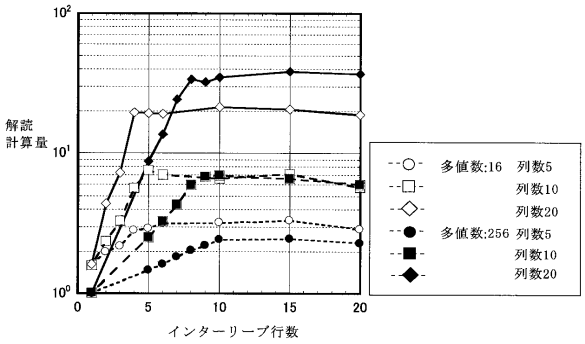
【図１６】



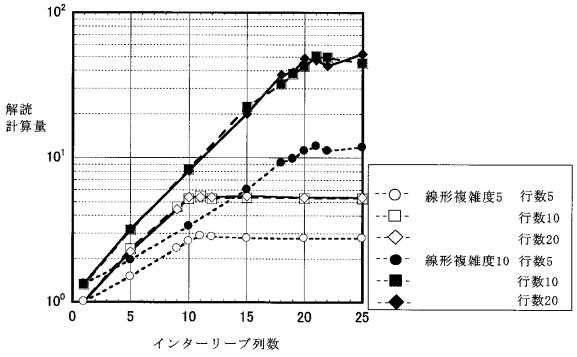
【図１７】



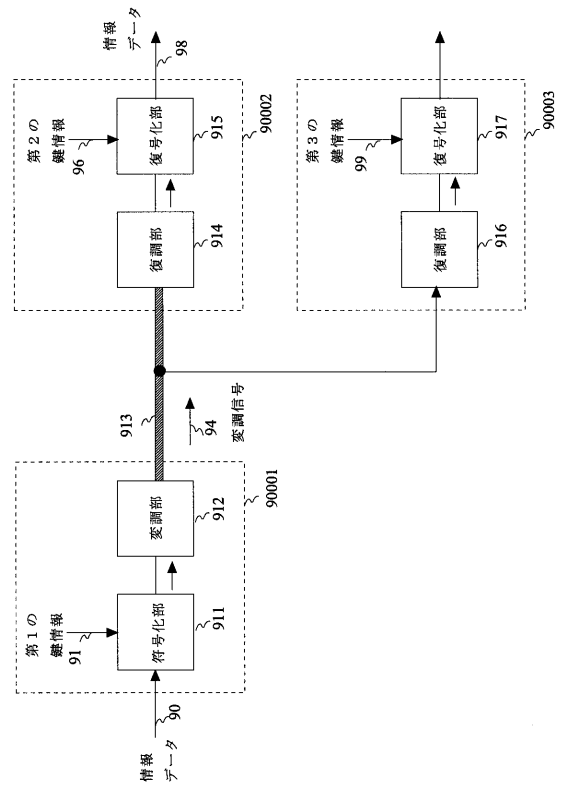
【図１８】



【図１９】



【図２０】



フロントページの続き

(72)発明者 生島 剛
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

審査官 中里 裕正

(56)参考文献 特開平１０－３２７１４１（ＪＰ，Ａ）
特開２００２－１１１６６０（ＪＰ，Ａ）
特開２００５－５７３１３（ＪＰ，Ａ）
生島 剛 Tsuyoshi Ikushima, 電子情報通信学会２００５年通信ソサイエティ大会講演論文集２ PROCEEDINGS OF THE 2005 IEICE COMMUNICATIONS SOCIETY CONFERENCE
広田 修 Osamu HIROTA, 光通信量子暗号Ｙ－００への攻撃は真の攻撃か？Ｐａｒｔ ＩＩ Are attacks on Y-00(Optical Communication Quantum Cryptography) the true attacks? Part-II, 電子情報通信学会技術研究報告 Ｖｏｌ．１０５ Ｎｏ．２９０ IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, 第105巻
今福 健太郎 Kentaro IMAFUKU, Ｙ－００プロトコルが古典的なストリーム暗号と等価であることについて Critical cryptoanalysis for Y-00, 電子情報通信学会技術研究報告 Ｖｏｌ．１０５ Ｎｏ．１９４ IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, 第105巻
広田 修 Osamu HIROTA, 光通信量子暗号（Ｙ－００）への攻撃は真の攻撃か？ Ｐａｒｔ Ｉ Are attacks on Y-00 (Optical Communication Quantum Cryptography) the true attacks? Part-I, 電子情報通信学会技術研究報告 Ｖｏｌ．１０４ Ｎｏ．７３２ IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, 第104巻

(58)調査した分野(Int.Cl., ＤＢ名)
H04K 1/00
H04L 9/20
JSTPlus/JMEDPlus/JST7580(JDreamII)