(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5052256号
(P5052256)
(45)発行日　平成24年10月17日(2012.10.17)　(24)登録日　平成24年8月3日(2012.8.3)

(51)Int.Cl.　　F I
H04K 1/02 (2006.01)　　H04K 1/02
H04L 9/12 (2006.01)　　H04L 9/00　631

請求項の数 7　(全 26 頁)

(21)出願番号　特願2007-209857(P2007-209857)
(22)出願日　平成19年8月10日(2007.8.10)
(65)公開番号　特開2008-206127(P2008-206127A)
(43)公開日　平成20年9月4日(2008.9.4)
審査請求日　平成22年3月24日(2010.3.24)
(31)優先権主張番号　特願2006-233504(P2006-233504)
(32)優先日　平成18年8月30日(2006.8.30)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2007-14279(P2007-14279)
(32)優先日　平成19年1月24日(2007.1.24)
(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】データ通信装置及びデータ通信方法

(57)【特許請求の範囲】
【請求項１】
所定の鍵情報を用いて情報データを暗号化し、データ受信装置との間で秘密通信を行うデータ送信装置であって、
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、
前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部を構成に含む多値符号変換部と、
前記情報データと前記変換後多値符号列とを合成し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理部と、
前記多値信号を所定の変調形式で変調して、変調信号として出力する変調部とを備え、
前記多値符号変換部は、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、
前記鍵情報は複数の鍵情報であって、
前記多値符号発生部は、前記複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、
前記多値符号変換部は、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補

が２つ以上となり、
前記累積部は、前記累積多値符号列の（ｋ－１）番目の値を所定数倍した値に、前記多値符号列のｋ番目の値を加算して、当該加算した値を前記累積多値符号列のｋ番目の値とすることを特徴とする、データ送信装置。
【請求項２】
所定の鍵情報を用いて情報データを暗号化し、データ受信装置との間で秘密通信を行うデータ送信装置であって、
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、
前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部を構成に含む多値符号変換部と、
前記情報データと前記変換後多値符号列とを合成し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理部と、
前記多値信号を所定の変調形式で変調して、変調信号として出力する変調部とを備え、
前記多値符号変換部は、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、
前記鍵情報は複数の鍵情報であって、
前記多値符号発生部は、前記複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、
前記多値符号変換部は、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補が２つ以上となり、
前記累積部は、前記累積多値符号列の（ｋ－１）番目の値を所定数倍した値に前記多値符号列のｋ番目の値を加算した値を、所定値で割った剰余を、前記累積多値符号列のｋ番目の値とすることを特徴とする、データ送信装置。
【請求項３】
所定の鍵情報を用いて情報データを暗号化し、データ受信装置との間で秘密通信を行うデータ送信装置であって、
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、
前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部を構成に含む多値符号変換部と、
前記情報データと前記変換後多値符号列とを合成し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理部と、
前記多値信号を所定の変調形式で変調して、変調信号として出力する変調部とを備え、
前記多値符号変換部は、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、
前記鍵情報は複数の鍵情報であって、
前記多値符号発生部は、前記複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、
前記多値符号変換部は、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補が２つ以上となり、
前記累積部は、前記累積多値符号列の（ｋ＋１）番目の値を、前記累積多値符号列のｋ番目の値とすることを特徴とする、データ送信装置。
【請求項４】

前記多値符号列の多値数は、前記変調信号を受信した際に重畳される外乱成分の分布幅に存在する多値レベルの数量の２乗以下とすることを特徴とする、請求項１ないし３のいずれかに記載のデータ送信装置。

【請求項５】

所定の鍵情報を用いて暗号化された情報データを受信し、データ送信装置との間で秘密通信を行うデータ受信装置であって、

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、

前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部を構成に含む多値符号変換部と、

前記送信装置から受信した変調信号を所定の復調方式で復調し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号として出力する復調部と、

前記変換後多値符号列に基づいて、前記多値信号から前記情報データを識別する識別部とを備え、

前記多値符号変換部は、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、

前記鍵情報は複数の鍵情報であって、

前記多値符号発生部は、前記複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、

前記多値符号変換部は、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補が２つ以上となり、

前記累積部は、前記累積多値符号列の（ｋ－１）番目の値を所定数倍した値に、前記多値符号列のｋ番目の値を加算して、当該加算した値を前記累積多値符号列のｋ番目の値とすることを特徴とする、データ受信装置。

【請求項６】

所定の鍵情報を用いて情報データを暗号化し、データ受信装置との間で秘密通信を行うデータ送信装置が実行するデータ送信方法であって、

前記データ送信装置の多値符号発生部によって、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ステップと、

前記データ送信装置の多値符号変換部によって、前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する多値符号変換ステップと、

前記データ送信装置の多値処理部によって、前記情報データと前記変換後多値符号列とを合成し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理ステップと、

前記データ送信装置の変調部によって、前記多値信号を所定の変調形式で変調して、変調信号として出力する変調ステップとを備え、

前記多値符号変換ステップにおいて、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、

前記多値符号発生ステップにおいて、前記複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、

前記多値符号変換ステップにおいて、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補が２つ以上となり、前記累積多値符号列の（ｋ－１）番目の値を所定数倍した値に、前記多値符号列のｋ番目の値を加算して、当該加算した値を前記累積多値符号列のｋ番目の値とすることを特徴とする、データ送信方法。

【請求項７】

所定の鍵情報を用いて暗号化された情報データを受信し、データ送信装置との間で秘密通信を行うデータ受信装置が実行するデータ受信方法であって、
前記データ受信装置の多値符号発生部によって、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ステップと、
前記データ受信装置の多値符号変換部によって、前記多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する多値符号変換ステップと、
前記データ受信装置の復調部によって、前記送信装置から受信した変調信号を所定の復調方式で復調し、前記情報データと前記変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号として出力する復調ステップと、
前記データ受信装置の識別部によって、前記変換後多値符号列に基づいて、前記多値信号から前記情報データを識別する識別ステップとを備え、
前記多値符号変換ステップは、前記変換後多値符号列が前記多値符号列の写像とならないように、前記多値符号列を非可逆変換し、
前記多値符号変換ステップにおいて、前記複数の多値符号列に対して四則演算または論理演算を含む数理処理を施すことにより、前記複数の多値符号列を前記変換後多値符号列に変換し、前記変換後多値符号列に基づいて前記多値符号列を逆算した場合に、前記多値符号列の候補が２つ以上となり、前記累積多値符号列の（ｋ－１）番目の値を所定数倍した値に、前記多値符号列のｋ番目の値を加算して、当該加算した値を前記累積多値符号列のｋ番目の値とすることを特徴とする、データ受信方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、第三者による傍受（盗聴等）を防ぐ暗号通信を行う装置及び方法に関し、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）方式を設定してデータ通信を行うデータ通信装置及びデータ通信方法に関する。

【背景技術】

【０００２】

従来、特定者同士でのみ通信を行うためには、送信側と受信側との間で伝送すべき情報データである平文を数学的に演算（符号化）及び逆演算（復号化）するための元情報（以下、鍵情報という）を共有することによって暗号通信を実現する構成が一般的に採用されている。

【０００３】

これに対して、近年、伝送路における物理現象を積極的に利用した暗号方式がいくつか提案されている。その方式の１つとして、伝送路で発生する量子雑音を利用して暗号通信を行うＹ－００プロトコルと呼ばれる方式がある。

【０００４】

図１５は、特許文献１に示された、Ｙ－００プロトコルを用いた従来のデータ通信装置９の構成例を示すブロック図である。以下では、特許文献１に示されている従来のデータ通信装置９の構成及び動作について説明する。図１５に示す通り、従来のデータ通信装置９は、送信部９０１と、受信部９０２と、伝送路９１０とで構成される。送信部９０１は、多値符号発生部９１１と、多値処理部９１２と、変調部９１３とで構成される。受信部９０２は、多値符号発生部９１４と、復調部９１５と、識別部９１６とで構成される。なお、盗聴受信部９０３は、傍受者が用いる装置であり、従来のデータ通信装置９を構成するものではない。

【０００５】

まず、送信部９０１と受信部９０２とは、予め同じ内容の鍵情報である鍵情報９１と鍵情報９６とをそれぞれ保持しておく。以下では、まず、送信部９０１の動作について説明する。多値符号発生部９１１は、鍵情報９１に基づいて、“０”から“Ｍ－１”（Ｍは、２以上の整数）までのＭ個の値を有する多値の疑似乱数系列である多値符号列９２を、擬似乱数発生器を用いて生成する。多値処理部９１２は、受信部９０２へ送信する情報デー

タ９０及び多値符号列９２に基づいて、以下に説明する信号フォーマットを用いて強度変調信号である多値信号９３を生成する。

【０００６】

図１６は、多値処理部９１２が用いる多値信号の信号フォーマットを示す図である。図１６に示す通り、多値符号列９２がＭ個の場合には、信号強度を２Ｍ個の信号強度レベル（以下、単に、レベルという）に分ける。そして、これらのレベルをＭ個のペア（以下、変調ペアという）にして、各変調ペアの一方のレベルに情報データ９０の値“０”を割り当て、他方のレベルに情報データ９０の値“１”を割り当てる。ここで、一般に、情報データ９０の値が“０”のレベルと、情報データ９０の値が“１”のレベルとを、２Ｍ個のレベル全体で均等に分布するように割り当てる。図１６では、偶数番目の変調ペアの低い方のレベルには“０”を割り当てて高い方のレベルには“１”を割り当てる一方で、奇数番目の変調ペアの低い方のレベルには“１”を割り当てて高い方のレベルには“０”を割り当てることによって、２Ｍ個のレベルに、情報データ９０の値“０”と“１”とを交互に割り当てている。

【０００７】

多値処理部９１２は、入力した多値符号列９２の各値に対応した変調ペアを選択した後に、情報データ９０の値に対応する、変調ペアの一方のレベルを選択し、その選択したレベルを有する多値信号９３を出力する。変調部９１３は、多値処理部９１２が出力した多値信号９３を強度変調信号である変調信号９４に変換し、伝送路９１０を介して受信部９０２へ伝送する。（なお、特許文献１では、第１の多値符号発生部９１１は「送信用疑似乱数発生部」、多値処理部９１２は「変調方式指定部」及び「レーザ変調駆動部」、変調部９１３は「レーザダイオード」、復調部９１５は「フォトディテクタ」、第２の多値符号発生部９１４は「受信用疑似乱数発生部」、識別部９１６は「判定回路」と記載されている。）

【０００８】

次に、受信部９０２の動作について説明する。復調部９１５は、伝送路９１０を介して伝送された変調信号９４を復調し、多値信号９５として出力する。多値符号発生部９１４は、鍵情報９６に基づいて、多値符号列９２と同じ多値の疑似乱数系列である多値符号列９７を生成する。識別部９１６は、多値符号発生部９１４から入力した多値符号列９７の各値によって、多値信号９５に用いられている各変調ペアを判断する。そして、識別部９１６は、判断した変調ペア及び復調部９１５から入力した多値信号９５を用いて、２値識別を行い、情報データ９０と等しい情報データ９８を得る。

【０００９】

図１７は、従来のデータ通信装置９の動作について具体的に説明するための図である。以下では、図１７を参照して、多値符号列９２が４値（Ｍ＝４）の場合の従来のデータ通信装置９の動作について具体的に説明する。図１７（ａ）及び（ｂ）に示す通り、情報データ９０の値が｛０，１，１，１｝、多値符号列９２の値が｛０，３，２，１｝に変化する場合を一例として説明する。この場合には、送信部９０１の多値信号９３のレベルは、図１７（ｃ）に示すように｛０，３，６，１｝と変化する。

【００１０】

具体的には、図１７（ｃ）に示すｔ１の期間では、多値符号列９２の値“０”に対応した第０の変調ペア（レベル０とレベル４とのペア）が選択される。その後に、情報データ９０の値“０”に対応する、第０の変調ペアのレベル０が選択され、この選択されたレベル０がｔ１における多値信号９３のレベルとなる。同様に、ｔ２の期間では、多値符号列９２の値“３”に対応した第３の変調ペア（レベル３とレベル７とのペア）が選択される。その後に、情報データ９０の値“１”に対応する、第３の変調ペアのレベル３が選択され、この選択されたレベル３がｔ２における多値信号９３のレベルとなる。ｔ３及びｔ４の期間においても同様に多値信号９３のレベルが設定される。この様に、多値符号列９２の値が偶数であるｔ１及びｔ３の期間では、変調ペアの低い方のレベルが情報データの“０”に対応して高い方のレベルが情報データの“１”に対応し、多値符号列９２の値が奇

数であるｔ２及びｔ４の期間では、変調ペアの低い方のレベルが情報データの“１”に対応して高い方のレベルが情報データの“０”に対応している。

【００１１】

次に、受信部９０２の識別部９１６に入力される多値信号９５は、図１７（ｅ）に示すように変化し、復調部９１５で変調信号９４が復調される際に発生するショット雑音等の雑音（外乱成分）を含んだ信号である。識別部９１６は、多値符号列９２と等しい多値符号列９７（図１７（ｄ）を参照）の各値に対応する各変調ペアを選択し、図１７（ｅ）に示すように、当該各変調ペアの中間のレベルをそれぞれ識別レベルとして設定する。そして、識別部９１６は、多値信号９５が識別レベルよりも高いか低いかを判断する。

【００１２】

具体的には、図１７（ｅ）に示すｔ１の期間では、識別部９１６は、多値符号列９７の値“０”に対応した第０の変調ペア（レベル０とレベル４とのペア）を選択し、第０の変調ペアの中間のレベル２を識別レベルとして設定する。そして、識別部９１６は、ｔ１において、多値信号９５が概ね識別レベルより低いレベルに分布しているので、多値信号９５は当該識別レベルよりも低いと判断する。同様に、ｔ２の期間では、識別部９１６は、多値符号列９７の値“３”に対応した第３の変調ペア（レベル３とレベル７とのペア）を選択し、第３の変調ペアの中間のレベル５を識別レベルとして設定する。そして、識別部９１６は、ｔ２において、多値信号９５が概ね識別レベルより低いレベルに分布しているので、多値信号９５は当該識別レベルよりも低いと判断する。ｔ３及びｔ４の期間においても同様に識別が行われ、識別部９１６の２値識別結果は、“低，低，高，低”となる。

【００１３】

次に、多値符号列９７の値が偶数の場合（ｔ１及びｔ３の期間の場合）には、識別部９１６は、選択した変調ペアの低い方のレベルを“０”と判断し、高い方のレベルを“１”と判断して、判断した値を情報データ９８として出力する。一方で、多値符号列９７の値が奇数の場合（ｔ２及びｔ４の期間の場合）には、識別部９１６は、選択した変調ペアの低い方のレベルを“１”と判断し、高い方のレベルを“０”と判断して、判断した値を情報データ９８として出力する。すなわち、多値符号列９７の値は、｛０，３，２，１｝であり“偶，奇，偶，奇”（但し、偶は偶数を示し、奇は奇数を示す）であるので、識別部９１６は、情報データ９０と等しい情報データ９８である｛０，１，１，１｝を出力する（図１７（ｆ）を参照）。この様にして、識別部９１６は、多値符号列９７の値が偶数か奇数かに応じて多値信号９５から、情報データ９８を得ることができる。

【００１４】

なお、以上では、多値符号列９７の値が偶数か奇数かに応じて、変調ペアの高い方及び低い方のレベルに割り当てる情報データの値が異なる信号フォーマット（図１６を参照）を使用する場合について具体的に説明した。しかし、信号フォーマットはこれには限られず、例えば、変調ペアの高い方のレベルに情報データ“１”が常に割当てられ、低い方のレベルに情報データ“０”が常に割当てられる信号フォーマットを使用してもよい。

【００１５】

また、既に述べた通り、多値信号９５には、復調部９１５で変調信号９４が復調される際に発生するショット雑音などの雑音が含まれているが、レベルの間隔（以下、ステップ幅という）等を適切に設定することで、２値識別における誤りの発生は無視できる程度に抑えることができる。

【００１６】

次に、想定される盗聴（傍受を含む）について説明する。図１５に示す通り、盗聴者は、盗聴受信部９０３を用いて、送信者と受信者とが共有する鍵情報を持たない状態で、変調信号９４から情報データ９０又は鍵情報９１の解読を試みる。盗聴受信部９０３は、復調部９２１と多値識別部９２２と解読処理部９２３とで構成され、伝送路９１０に接続されている。

【００１７】

ここで、盗聴者が正規受信者（受信部９０２）と同様の２値識別を行う場合には、盗聴

者は鍵情報を持たないために、鍵情報が取り得る全ての値に対して識別を試みる必要がある。しかし、この方法は、識別試行回数が鍵情報の長さの増加に伴い指数関数的に増大するために、鍵情報の長さが十分長い場合には現実的ではない。

【００１８】

そこで、より効率的な方法として、盗聴者は、復調部９２１で変調信号９４を復調して得られる多値信号８１を多値識別部９２２で多値識別し、得られた受信系列８２に対して解読処理部９２３によって解読処理を行うことで、情報データ９０若しくは鍵情報９１の解読を試みると考えられる。このような解読方法を用いた場合、仮に、盗聴受信部９０３が多値信号９３を受信系列８２として誤り無く受信（識別）することができれば、受信系列８２を用いて１回の試行で鍵情報９１の解読を行うことが可能となる。

【００１９】

ここで、復調部９２１で変調信号９４が復調される際に発生するショット雑音（外乱成分）が変調信号９４に重畳されるので、当該ショット雑音は、多値信号８１に含まれることになる。このショット雑音は、量子力学の原理により必ず発生することが知られている。このことから、多値信号９３のステップ幅をショット雑音の分布幅よりも十分小さくしておけば、雑音を含む多値信号８１は、正しいレベル（多値信号９３のレベル）ではない様々なレベルに渡り分布することとなる。例えば、図１７（ｇ）に示すように、ｔ２において、多値信号８１は、レベル２～４に渡って分布している。従って、盗聴者は、正しいレベルが、識別によって得られた受信系列８２のレベルではない可能性（識別誤りの可能性）を考慮した解読処理を行う必要がある。このため、識別誤りが無い場合と比較して、解読処理に要する試行回数（以下、受信可能性数という）、すなわち計算量は増大することとなる。この結果として、盗聴に対する安全性は向上する。

【特許文献１】特開２００５－５７３１３号公報

【発明の開示】

【発明が解決しようとする課題】

【００２０】

しかしながら、上述した従来のデータ通信装置９には、以下に説明する問題がある。復調部９２１で変調信号９４を復調する際に発生するショット雑音（外乱成分）の分布幅は小さいために、盗聴者による多値識別誤りのレベルは、多値信号９３（正規の信号）のレベルの近傍のみに発生する。例えば、図１７（ｇ）のｔ２の期間では、多値信号９３のレベルは３であるが、盗聴者が誤る可能性のあるレベルは２又は４に限られる。このことから、盗聴者は、自己が受信したレベルの近傍に正規の信号のレベルが存在することを前提に解読処理を行うことができる。この結果として、従来のデータ通信装置９では、盗聴者が解読処理に要する受信可能性数は小さくなるので、暗号通信の十分な安全性を確保できなくなる。

【００２１】

図１８は、図１５に示す従来のデータ通信装置９における受信可能性数を説明するための図である。図１９は、図１８（ｃ）に示す多値信号９３を説明するための図である。以下では、図１８及び図１９を参照して、従来のデータ通信装置９の受信可能性数について説明する。図１８（ａ）及び（ｂ）に示す通り、送信部９０１の多値処理部９１２に入力される情報データ９０が｛１，０，１，１｝であり、多値数Ｍが８である多値符号列９２が｛４，１，４，２｝である場合を一例に挙げて説明する。この場合、図１５に示す多値処理部９１２は、図１６に示す信号フォーマットに従って、多値信号９３として｛１２，９，１２，１０｝を生成する（図１８（ｃ）及び図１９を参照）。多値信号９３｛１２，９，１２，１０｝は、変調部９１３で変調され、変調信号９４として伝送路９１０を介して伝送される。

【００２２】

盗聴者は、復調部９２１（図１５の盗聴受信部９０３を参照）を用いて伝送路９１０上の変調信号９４を復調して、多値信号８１を得る。既に説明した様に、多値信号８１には外乱成分であるショット雑音が混入しているので、多値識別部９２２において多値識別誤

りが生じる可能性がある。ここで、この多値識別誤りの影響によって多値識別部９２２が識別する可能性のあるレベルの数量を、以下では「識別可能数Ｊ」という。一例として、多値識別の結果、多値識別部９２２が正規のレベル（多値信号９３のレベル）及び当該正規のレベルの上下に隣接するレベルの合計３通りに識別をする可能性がある場合、つまり、識別可能数Ｊ＝３の場合について説明する。この場合、盗聴者が多値識別の結果として得る受信系列８２は、例えば｛１１，１０，１３，１０｝となる（図１８（ｄ）を参照）。この受信系列８２を用いて盗聴者が正規の信号（多値信号９３）の解読を試みる場合、盗聴者は、識別可能数Ｊに基づいて正規の信号を推測し、続いて、図１６に示す信号フォーマットを用いて多値符号列９２を導出し、導出した多値符号列９２を用いて鍵情報９１の特定を試みると考えられる。

【００２３】

具体的には、盗聴者は、識別可能数Ｊ＝３であることを考慮して、送信された正規の信号である多値信号９３の値が、｛１０～１２，９～１１，１２～１４，９～１１｝の範囲のいずれかの値であると推測できる。そして、盗聴者は、図１６の信号フォーマットを用いて、送信部９０１で用いられた多値符号列９２の値が、｛２～４，１～３，４～６，１～３｝の範囲のいずれかの値であると推測できる。そして、盗聴者は、多値符号列９２が取り得る値を、「３通り×３通り×３通り×３通り＝８１通り」の値に絞り込むことができる。このことから、盗聴者が多値符号列９２を解読するために行う処理の試行回数は、計３×３×３×３＝８１通りとなる。つまり、従来のデータ通信装置９における受信可能性数は、８１である。

【００２４】

以上に説明した通り、盗聴受信部９０３において、復調部９２１で生じるショット雑音の分布幅は小さいので、多値識別部９２２で多値識別誤りが生じる可能性のあるレベルの範囲は或る程度限定される。そして、従来のデータ通信装置９では、盗聴者が多値符号列９２を解読するための受信可能性数は小さいので、暗号通信における十分な安全性を確保できない。

【００２５】

それ故に、本発明の目的は、受信可能性数を増加させることによって、暗号通信における高い安全性を確保できるデータ通信装置及びデータ通信方法を提供することである。

【課題を解決するための手段】

【００２６】

本発明は、所定の鍵情報を用いて情報データを暗号化し、受信装置との間で秘密通信を行うデータ送信装置に向けられている。そして、上記目的を達成するために、本発明のデータ送信装置は、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、多値符号列を変換後多値符号列に変換する多値符号変換部と、情報データと変換後多値符号列とを合成し、情報データと変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理部と、多値信号を所定の変調形式で変調して、変調信号として出力する変調部とを備える。ただし、多値符号変換部は、変換後多値符号列が多値符号列の写像とならないように、多値符号列を非可逆変換する。

【００２７】

これによって、盗聴者が復調した多値信号を元に、正しい変換後多値符号列を偶発的に取得できたとしても、変換後多値符号列を元に多値符号列を逆算し、鍵情報の特定に遡る処理を困難化することができる。

【００２８】

また、鍵情報は複数の鍵情報であってもよい。この場合、多値符号発生部は、複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、多値符号変換部は、複数の多値符号列を変換後多値符号列に変換する。

【００２９】

好ましくは、多値符号変換部は、多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部によって構成される。累積部は、累積多値符号列

の（ｋ－１）番目の値を所定数倍した値に、多値符号列のｋ番目の値を加算して、当該加算した値を累積多値符号列のｋ番目の値とする。

【００３０】

また、累積部は、累積多値符号列の（ｋ－１）番目の値を所定数倍した値に多値符号列のｋ番目の値を加算した値を、所定値で割った剰余を、累積多値符号列のｋ番目の値としてもよい。あるいは、累積部は、累積多値符号列の（ｋ＋１）番目の値を、累積多値符号列のｋ番目の値として出力してもよい。

【００３１】

好ましくは、多値符号列の多値数は、変調信号を受信した際に重畳される外乱成分の分布幅に存在する多値レベルの数量の２乗以下とする。

【００３２】

また、本発明は、所定の鍵情報を用いて暗号化された情報データを受信し、送信装置との間で秘密通信を行うデータ受信装置にも向けられている。そして、上記目的を達成するために、本発明のデータ受信装置は、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、多値符号列を変換後多値符号列に変換する多値符号変換部と、送信装置から受信した変調信号を所定の復調方式で復調し、情報データと変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号として出力する復調部と、変化後多値符号列に基づいて、多値信号から情報データを識別する識別部とを備える。ただし、多値符号変換部は、変換後多値符号列が多値符号列の写像とならないように、多値符号列を非可逆変換する。

【００３３】

また、鍵情報は複数の鍵情報であってもよい。この場合、多値符号発生部は、複数の鍵情報から信号レベルが略乱数的に変化する複数の多値符号列を発生し、多値符号変換部は、複数の多値符号列を変換後多値符号列に変換する。

【００３４】

好ましくは、多値符号変換部は、多値符号列に含まれる値を累積した累積多値符号列を変換後多値符号列として生成する累積部によって構成される。累積部は、累積多値符号列の（ｋ－１）番目の値を所定数倍した値に、多値符号列のｋ番目の値を加算して、当該加算した値を累積多値符号列のｋ番目の値とする。

【００３５】

また、上述したデータ送信装置が備える各構成は、所定の鍵情報を用いて情報データを暗号化し、受信装置との間で秘密通信を行うデータ送信方法としても捉えることができる。すなわち、データ送信方法は、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ステップと、多値符号列を変換後多値符号列に変換する多値符号変換ステップと、情報データと変換後多値符号列とを合成し、情報データと変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号を生成する多値処理ステップと、多値信号を所定の変調形式で変調して、変調信号として出力する変調ステップとを備え、多値符号変換ステップは、変換後多値符号列が多値符号列の写像とならないように、多値符号列を非可逆変換する、方法である。

【００３６】

また、同様に、上述したデータ受信装置が備える各構成は、所定の鍵情報を用いて暗号化された情報データを受信し、送信装置との間で秘密通信を行うデータ受信方法としても捉えることができる。すなわち、データ受信方法は、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ステップと、多値符号列を変換後多値符号列に変換する多値符号変換ステップと、送信装置から受信した変調信号を所定の復調方式で復調し、情報データと変換後多値符号列との組み合わせに対応した複数のレベルを有する多値信号として出力する復調ステップと、変化後多値符号列に基づいて、多値信号から情報データを識別する識別ステップとを備え、多値符号変換ステップは、変換後多値符号列が多値符号列の写像とならないように、多値符号列を非可逆変換する、方法である。

【発明の効果】

【００３７】
以上のように、本発明のデータ通信装置及びデータ通信方法によれば、多値符号変換部が多値符号列を非可逆変換して、変換後多値符号列を生成することで、盗聴者が変換後多値符号列から想定する多値符号列のパターン数を増大させることができる。これによって、暗号文の解読に要する時間を増大させ、秘匿性の高いデータ通信を実現することができる。
【００３８】
また、本発明のデータ通信装置及びデータ通信方法によれば、複数の多値符号発生部を備えることで、多値符号変換部が複数の多値符号列から変換後多値符号列を生成するので、変換後多値符号列の生成速度が低下しない。これによって、情報データの伝送レートが、変換後多値符号列の生成速度に応じて制限されることを防止することができる。
【００３９】
また、本発明のデータ通信装置及びデータ通信方法によれば、多値符号変換部を累積部で構成することによって、盗聴者の受信時に発生する多値識別誤りの効果（可能性）を増加することができるので、暗号解読において考慮すべき受信可能性が増加する。この結果として、暗号通信における高い安全性を確保できる。
【００４０】
本発明のこれらおよび他の目的、特徴、局面、効果は、添付図面と照合して、以下の詳細な説明から一層明らかになるであろう。
【発明を実施するための最良の形態】
【００４１】
（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１の構成例を示すブロック図である。図１において、データ通信装置１は、データ送信装置１０１（以下、送信部１０１と記す）と、データ受信装置２０１（以下、受信部２０１と記す）とが、伝送路１１０を介して接続された構成である。送信部１０１は、多値符号発生部１１１と、多値符号変換部１１２と、多値処理部１１３と、変調部１１４とを備える。受信部２０１は、多値符号発生部２１１と、多値符号変換部２１２と、識別部２１４と、復調部２１３とを備える。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が用いられる。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ことが可能な自由空間であってもよい。また、送信部１０１は鍵情報１１を予め保持し、受信部２０１は鍵情報２１を予め保持しており、鍵情報１１と鍵情報２１とは同じ内容の鍵情報である。
【００４２】
送信部１０１において、多値符号発生部１１１は、鍵情報１１に基づいて、“０”から“Ｍ－１”までのＭ個の値を有する多値の疑似乱数系列である多値符号列１２を発生する。多値符号列１２は、多値符号変換部１１２に入力される。多値符号変換部１１２は、多値符号列１２を所定の規則に従って非可逆変換し、変換後多値符号列１３として出力する。ここで非可逆変換とは、多値符号列１２と変換後多値符号列１３とが１対１に対応しない変換をいう。すなわち、変換後多値符号列１３は、多値符号列１２の写像とならないことを特徴とする。
【００４３】
多値処理部１１３には、情報データ１０と、変換後多値符号列１３とが入力される。多値処理部１１３は、所定の手順に従って、情報データ１０と変換後多値符号列１３とを合成し、情報データ１０と変換後多値符号列１３との組み合わせに対応したレベルを有する多値信号１４を生成する。変調部１１４は、多値信号１４を所定の変調形式で変調して、変調信号１５として伝送路１１０に送出する。ここで、所定の変調形式とは、例えば、振幅変調、周波数変調、位相変調、及び光強度変調などの形式である。
【００４４】
受信部２０１において、復調部２１３は、伝送路１１０を介して伝送されてきた変調信

号１５を所定の復調方式で復調し、多値信号２４を再生する。ここで、所定の復調形式とは、変調部１１４の変調形式に対応した形式である。多値符号発生部２１１は、鍵情報２１に基づいて、多値の疑似乱数系列である多値符号列２２を発生する。なお、多値符号発生部２１１の動作は、送信部１０１が備える多値符号発生部１１１と同様である。多値符号変換部２１２は、多値符号列２２を所定の規則に従って非可逆変換し、変換後多値符号列２３として出力する。なお、多値符号変換部２１２の動作は、送信部１０１が備える多値符号変換部１１２と同様である。識別部２１４は、変換後多値符号列２３に基づいて、多値信号２４の識別（２値判定）を行い、当該識別結果を情報データ２０として出力する。

【００４５】

次に、従来構成の課題である、盗聴者が正しい多値信号１４，２４のレベルを長期に亘って偶発的に取得し、数理アルゴリズムを利用して鍵情報１１，２１を特定する場合を考える。このとき盗聴者が行う鍵情報特定までの手順は以下のようになる。盗聴者は、まず最初に、受信した多値信号１４，２４のレベルを元に、変換後多値符号列１３，２３の特定を試みる。続いて、変換後多値符号列１３，２３を逆算して、多値符号列１２，２２の特定を試みる。最後に、多値符号列１２，２２に対して擬似乱数列を特定する数理アルゴリズムを適用し、鍵情報１１，２１の特定を試みる。しかしながら、本発明では、多値符号列１２，２２から変換後多値符号列１３，２３を生成する変換処理が非可逆であるため、盗聴者は、変換後多値符号列１３，２３から多値符号列１２，２２の逆算を一意に行えない。

【００４６】

ここで、非可逆な変換処理による変換後多値符号列１３，２３の生成過程を図２Ａを用いて説明する。ただし、多値符号変換部１１１及び多値符号変換部２１２は、同様の動作を行うため、ここでは多値符号変換部１１１が変換後多値符号列１３を生成する過程を代表して説明する。図２Ａは、非可逆な変換処理による変換後多値符号列１３の生成過程の一例を示す図である。ただし、多値符号列１２の多値数を８（Ｍ＝８）とした。図２Ａを参照して、多値符号変換部１１１は、例えば、７シンボルの多値符号列１２｛０，１，２，３，４，５，６｝から所定の値を減算し（ここでは３を減算し）、３を減算した多値符号列１２の絶対値を求めることにより、変換後多値符号列１３｛３，２，１，０，１，２，３｝を生成する。

【００４７】

このとき、変換後多値符号列１３の値“３”に相当する多値符号列１２は、“０”或いは“６”、変換後多値符号列１３の値“２”に相当する多値符号列１２は、“１”或いは“５”の如く対応付けられる。受信部２０１（すなわち、正規受信者）は、同様の過程に従って、多値符号列２２から変換後多値符号列２３を生成するため、多値信号２４から情報データ２０の復号が可能となる。

【００４８】

ここで、盗聴者が多値信号１４から正しい変換後多値符号列１２を取得できたと仮定した場合の盗聴者による変換後多値符号列１３の解読処理について説明する。図２Ｂは、盗聴者による変換後多値符号列１３の解読処理を説明する図である。図２Ｂを参照して、盗聴者が想定する多値符号列１２の候補は、（｛０或いは６｝，｛１或いは５｝，｛２或いは４｝，３，｛２或いは４｝，｛１或いは５｝，｛０或いは６｝）の全ての組合せ（６４通り）となる。このため、盗聴者は、変換後多値符号列１３を解読して鍵情報１１を特定するには、これら６４通りの多値符号列１２に対して数理アルゴリズムを適用する必要があり、解読に要する計算量が増加する。

【００４９】

なお、上述した説明では、多値符号変換部１１２は、多値符号列１２を１シンボル毎に変換後多値符号列１３に変換したが、複数シンボル毎に変換後多値符号列１３に変換することも可能である。図３Ａは、複数シンボル毎に変換後多値符号列１３を生成する過程を説明する図である。ただし、多値符号列１２の多値数を８（Ｍ＝８）とした。図３Ａを参

照して、多値符号変換部１１２は、多値符号列１２｛６，３，７，２，５，１｝を２シンボルごとに加算し、変換後多値符号列１３｛９，９，６｝を生成する。受信部２０１（すなわち、正規受信者）は、同様の過程に従って、多値符号列２２から変換後多値符号列２３を生成するため、多値信号２４から情報データ２０の復号が可能となる。

【００５０】

ここで、盗聴者が多値信号１４から複数シンボル毎に生成された変換後多値符号列１３を取得できたと仮定した場合の盗聴者による変換後多値符号列１３の解読処理について説明する。図３Ｂは、盗聴者による複数シンボル毎に生成された変換後多値符号列１３の解読処理を説明する図である。図３Ｂを参照して、盗聴者が想定する多値符号列１２の候補は、変換後多値符号列１３の値“９”に対して、｛（２，７）、（３，６）、（４，５）、（５，４）、（６，３）、（７，２）｝の６通りが考えられ、変換後多値符号列１３の値“６”に対して、｛（０，６）、（１，５）、（２，４）、（３，３）、（４，２）、（５，１）、（６，０）｝の７通りが考えられる。従って、盗聴者は、鍵情報１１を特定するには、変換後多値符号列１３｛９，９，６｝に対して、６×６×７＝２５２通りの多値符号列１２の全パターンに対して数理アルゴリズムを適用する必要があり、さらに解読に要する計算量が増加する。

【００５１】

なお、変換後多値符号列１３の生成に利用する多値符号列１２のシンボル数を増加させることで、変換後多値符号列１３に対応する多値符号列１２のパターン数が増加するため、盗聴者の解読に要する計算量を増加させることができる。また、上述した説明では、多値符号列１２を加算することで、変換後多値符号列１３を生成したが、これに限定されるものではなく、四則演算、論理演算、その他数理処理により、非可逆性を確保できるものであればいかなるものでもよい。

【００５２】

また、上述した説明では、多値符号変換部１１２が多値符号列１２を複数シンボル毎に加算して、変換後多値符号列１３を生成する場合を説明したが、多値符号変換部１１２は、多値符号列１２を分岐し、分岐した一方の多値符号列に遅延を与えて、他方の多値符号列と合成することで、変換後多値符号列１３を生成してもよい。この場合、受信部２０１が備える多値符号変換部２１２も、多値符号変換部１１２と同様の動作を行うものとする。

【００５３】

以上のように、本発明の第１の実施形態に係るデータ通信装置１は、多値符号変換部１１２，２１２が多値符号列１２，２２を非可逆変換して、変換後多値符号列１３，２３を生成することで、盗聴者が変換後多値符号列１３，２３から想定する多値符号列１２，２２のパターン数を増大させることができる。これによって、暗号文の解読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を実現することができる。

【００５４】

また、データ通信装置１は、多値符号変換部１１２，２１２が多値符号列１２，２２を複数シンボル毎に変換後多値符号列１３，２３に変換することで、盗聴者が変換後多値符号列１３，２３から想定する多値符号列１２，２２のパターン数をさらに増大させることができる。これによって、暗号文の解読に要する時間を著しく増大させ、より秘匿性の高いデータ通信を実現することができる。

【００５５】

（第２の実施形態）

図４は、本発明の第２の実施形態に係るデータ通信装置２の構成例を示すブロック図である。なお以下では、第１の実施形態において説明した内容は省略し、第１の実施形態との差分を重点的に説明する。図４において、データ通信装置２は、データ送信装置１０２（以下、送信部１０２と記す）と、データ受信装置２０２（以下、受信部２０２と記す）とが、伝送路１１０を介して接続された構成である。送信部１０２は、第１から第ｎの多値符号発生部１１１－１～１１１－ｎと、多値符号変換部１１２と、多値処理部１１３と

、変調部１１４とを備える。受信部２０２は、第１から第ｎの多値符号発生部２１１－１～２１１－ｎと、多値符号変換部２１２と、識別部２１４と、復調部２１３とを備える。ただし、ｎは２以上の任意の整数である。

【００５６】

送信部１０２において、第１から第ｎの多値符号発生部１１１－１～１１１－ｎは、それぞれ第１から第ｎの鍵情報１１－１～１１－ｎに基づいて、第１から第ｎの多値符号列１２－１～１２－ｎを出力する。なお、第１から第ｎの多値符号発生部１１１－１～１１１－ｎをまとめた構成を１つの多値符号発生部であると考えることも可能である。この場合、多値符号発生部は、第１から第ｎの鍵情報１１－１～１１－ｎに基づいて、第１から第ｎの多値符号列１２－１～１２－ｎを出力する。

【００５７】

第１から第ｎの多値符号列１２－１～１２－ｎは、多値符号変換部１１２に入力される。多値符号変換部１１２は、第１から第ｎの多値符号列１２－１～１２－ｎを元に、変換後多値符号列１３を生成する。多値符号変換部１１２が変換後多値符号列１３を生成する方法は第１の実施形態で説明したものと同様である。ここで、複数の多値符号列１２－１～１２－ｎから変換後多値符号列１３を生成するメリットについて説明する。第１の実施形態では、複数シンボル毎に変換後多値符号列２３を生成した場合、変換後多値符号列２３の生成速度が低下し、情報データ１０の伝送レートが、変換後多値符号列２３の生成速度に制限される可能性があった。しかし、本実施形態では、多値符号変換部１１２は、第１から第ｎの多値符号列１２－１～１２－ｎを元に変換後多値符号列２３を生成することで、変換後多値符号列２３の生成速度が低下せず、情報データ１０の伝送レートが、変換後多値符号列２３の生成速度に制限されない。

【００５８】

また、受信部２０２においても、第１から第ｎの多値符号発生部２１１－１～２１１－ｎ、及び多値符号変換部２１２の動作は、送信部１０２と同様である。

【００５９】

さらに、本実施形態に係るデータ通信装置２ａは、上述した構成とは異なる構成にすることもできる。図５は、本発明の第２の実施形態に係るデータ通信装置２ａの構成例を示すブロック図である。図５に示すように、送信部１０２ａは、第１から第ｍ（ｍは整数、ｍ＜ｎ）の鍵情報１１－１～１１－ｍを、重複を許容して第１から第ｎの多値符号発生部１１１－１～１１１－ｎに入力することにより、暗号通信に利用する鍵情報の数を減らし、送受信間での鍵情報１１の共有を簡素化することが可能となる。

【００６０】

また、同一の鍵情報１１が入力される複数の多値符号発生部１１１は、同一の鍵情報１１に対してそれぞれ異なる多値符号列１２を出力することにより、多値符号発生部間の相関性をなくし、変換後多値符号列１３から各多値符号列１２の逆算過程を複雑化することが可能となる。また、受信部２０２ａにおいても同様に、鍵情報２１－１～２１－ｍの重複を許容することで、多値信号２４から情報データ２０の復号が可能となる。

【００６１】

以上のように、本発明の第２の実施形態に係るデータ通信装置２は、複数の多値符号発生部１１１－１～１１１－ｎを備え、多値符号変換部１１２が複数の多値符号列１２－１～１２－ｎから変換後多値符号列１３を生成するので、変換後多値符号列１３の生成速度が低下しない。これによって、情報データ１０の伝送レートが、変換後多値符号列１３の生成速度に制限されることを防止することができる。

【００６２】

なお、第１及び第２の実施形態に係る多値符号発生部１１１は、図６に示すような構成であってもよい。図６は、多値符号発生部１１１の構成の一例を示すブロック図である。図６において、多値符号発生部１１１は、２値乱数発生部１１１ｘと、多値化部１１１ｙとを含む。２値乱数発生部１１１ｘは、鍵情報１１から略乱数的に変化する２値乱数列を発生する。多値化部１１１ｙは、２値乱数列に所定の多値化処理を施し、多値符号列１２

を出力する。この構成により、多値符号発生部１１１は、多値化部１１１ｙにおける多値化処理の方法、すなわち２値乱数列と多値符号列１２とのマッピング方法を変えることで、多値符号列１２の多値数、及び同一の鍵情報１１に対して生成される多値符号列１２を変化させることが可能となる。

【００６３】

（第３の実施形態）

図７は、本発明の第３の実施形態に係るデータ通信装置３の構成例を示すブロック図である。図７に示す通り、データ通信装置３は、データ送信装置１０３（以下、送信部１０３という）と、データ受信装置２０３（以下、受信部２０３という）とが、伝送路１１０を介して接続された構成である。送信部１０３は、多値符号発生部１１１と、多値符号変換部１３２と、多値処理部１１３と、変調部１１４とを備える。受信部２０３は、多値符号発生部２１１と、多値符号変換部２３２と、復調部２１３と、識別部２１４とを備える。ただし、多値符号変換部１３２は累積部１３２１から構成され、多値符号変換部２３２は累積部２３２１から構成される。

【００６４】

以下では、データ通信装置３の動作について説明する。まず、送信部１０３の動作について説明する。多値符号発生部１１１は、鍵情報１１に基づいて”０”から”ｍ－１”（ｍは、２以上の整数）までのｍ個の値を有する多値の擬似乱数系列である多値符号列１２を発生する。多値符号列１２は、多値符号変換部１３２に入力される。多値符号変換部１３２において、累積部１３２１は、多値符号列１２に対して後に説明する累積処理を施し、得られた累積値を累積多値符号列１６として出力する。なお、本実施例では、累積多値符号列１６は、”０”から”Ｍ－１”（Ｍは、２以上の整数）のＭ個の値を有する多値符号列とする。多値処理部１１３には、送信部２０３へ送信する情報データ１０と、累積多値符号列１６とが入力される。多値処理部１１３は、図１６に示す信号フォーマットに従って、情報データ１０と累積多値符号列１６との組合せに対応したレベルを有する多値信号１４を生成する。変調部１１４は、多値信号１４を所定の変調形式で変調して変調信号１５を生成し、伝送路１１０に送出する。ここで、所定の変調形式とは、例えば、振幅変調、周波数変調、位相変調及び光強度変調等の変調形式である。

【００６５】

次に、受信部２０３の動作について説明する。復調部２１３は、伝送路１１０を介して伝送された変調信号１５を所定の復調形式で復調して、多値信号２４を再生する。ここで、所定の復調形式とは、変調部１１４の変調方式に対応した復調形式である。多値符号発生部２１１は、鍵情報２１に基づいて、”０”から”ｍ－１”（ｍは、２以上の整数）までのｍ個の値を有する擬似乱数系列である多値符号列２２を発生する。なお、多値符号発生部２１１の動作は、送信部１０３が備える多値符号発生部１１１の動作と同じである。多値符号列２２は、多値符号変換部２３２に入力される。多値符号変換部２３２において、累積部２３２１は、多値符号列２２に対して累積処理を施し、得られた累積値を累積多値符号列２６として出力する。なお、累積部２３２１の動作は、送信部１０３が備える累積部１３２１の動作と同じであり、本実施形態においては、累積多値符号列２６は、”０”から”Ｍ－１”のＭ個の値を有する多値符号列とする。識別部２１４は、累積多値符号列２６に基づいて、多値信号２４の識別（２値判定）を行い、当該識別結果を情報データ２０として出力する。

【００６６】

以下では、データ通信装置３が行う暗号通信を、盗聴者が解読する場合の受信可能性数（暗号通信の解読処理に要する試行回数）について、従来のデータ通信装置９（図１５参照）と比較して説明する。図８は、図７に示すデータ通信装置３における受信可能性数を説明するための図である。図９は、図８（ｄ）の多値信号１４について説明するための図である。図８（ａ）及び（ｂ）に示す通り、送信部１０３が備える多値処理部１１３に入力される情報データ１０が｛１，０，１，１｝であり、多値数ｍが８である多値符号列１２が｛４，１，４，２｝である場合を一例に挙げて説明する。

【００６７】
まず、累積部１３２１は、多値符号列１２｛４，１，４，２｝の各値を、順次累積して累積多値符号列１６｛４，５，９，１１｝を生成する。具体的には、累積部１３２１は、累積多値符号列１６の０番目の値“０”（０番目は存在しないので、０番目の値は０と考える）と多値符号列１２の１番目の値“４”との和である“４”を累積多値符号列１６の１番目の値とし、同様に、累積多値符号列１６の１番目の値“４”と多値符号列１２の２番目の値“１”との和である“５”を累積多値符号列１６の２番目の値とし、累積多値符号列１６の２番目の値“５”と多値符号列１２の３番目の値“４”との和である“９”を累積多値符号列１６の３番目の値とし、累積多値符号列１６の３番目の値“９”と多値符号列１２の４番目の値“２”との和である“１１”を累積多値符号列１６の４番目の値とする。つまり、累積多値符号列１６の１番目の値は“０＋４＝４”であり、累積多値符号列１６の２番目の値は“０＋４＋１＝５”であり、累積多値符号列１６の３番目の値は“０＋４＋１＋４＝９”であり、累積多値符号列１６の４番目の値は“０＋４＋１＋４＋２＝１１”である。ただし、多値符号列１２は、４つの値から成り、多値数ｍ＝８である。このことから、累積多値符号列１６の多値数Ｍは、“４×８＝３２”である。

【００６８】
次に、多値処理部１１３は、累積多値符号列１６｛４，５，９，１１｝と情報データ１０｛１，０，１，１｝とを入力し、図１６に示す信号フォーマットに従って、多値信号１４｛３６，３７，９，１１｝を生成する（図８（ｄ）及び図９を参照）。多値信号１４｛３６，３７，９，１１｝を生成する具体的な動作については、背景技術で説明した動作と同様であるので省略する。ここで、識別可能数Ｊ＝３と仮定した場合、盗聴者は、盗聴受信部９０３を用いて伝送路１１０上の変調信号１５を受信して多値識別を行い、受信系列８２として、例えば｛３５，３８，９，１１｝を得る（図８（ｅ）を参照）。そして、盗聴者は、識別可能数Ｊ＝３であることを考慮して、送信された正規の信号である多値信号１４の値が、｛３４～３６，３７～３９，８～１０，１０～１２｝の範囲のいずれかの値であると推測できる（図８（ｆ）を参照）。そして、盗聴者は、図１６の信号フォーマットを用いて、送信部１０３で用いられた累積多値符号列１６の値が、｛２～４，５～７，８～１０，１０～１２｝の範囲のいずれかの値であると推測できる（図８（ｇ）を参照）。

【００６９】
次に、盗聴者は、累積多値符号列１６の推測値｛２～４，５～７，８～１０，１０～１２｝を用いて多値符号列１２を導出するために、送信部１０３の累積部１３２１で行われた累積過程を逆算する必要がある。ここで、多値符号列１２の推測値を｛ｘ１，ｘ２，ｘ３，ｘ４｝と表す。但し、多値符号列１２の多値数ｍは８なので、ｘ１，ｘ２，ｘ３，ｘ４は、０～７の整数のいずれかである。この様に表すと、累積多値符号列１６の１番目の値”２～４”は、累積多値符号列１６の０番目の値“０”に“ｘ１”が加算されたものとなる。このことから、盗聴者は、ｘ１が”２～４”の範囲のいずれかの値であると推測できる。同様に、累積多値符号列１６の２番目の値”５～７”は、累積多値符号列１６の１番目の値“２～４”に“ｘ２”が加算されたものとなる。このことから、盗聴者は、ｘ２が”１～５”の範囲のいずれかの値であると推測できる。累積多値符号列１６の３番目の値”８～１０”は、累積多値符号列１６の２番目の値“５～７”に“ｘ３”が加算されたものとなる。このことから、盗聴者は、ｘ３が”１～５”の範囲のいずれかの値であると推測できる。累積多値符号列１６の４番目の値”１０～１２”は、累積多値符号列１６の３番目の値“８～１０”に“ｘ４”が加算されたものとなる。このことから、盗聴者は、ｘ４が”０～４”の範囲のいずれかの値であると推測できる。この様にして、盗聴者は、多値符号列１２の値が、｛２～４，１～５，１～５，０～４｝の範囲のいずれかの値であると推測できる（図８（ｈ）を参照）。

【００７０】
このことから、盗聴者は、多値符号列１２が取り得る値を、「３通り×５通り×５通り×５通り＝３７５通り」に絞り込むことができる。すなわち、盗聴者が多値符号列１２を

解読するために行う処理の試行回数は、計３×５×５×５＝３７５通りとなる（図８（ｉ）を参照）。つまり、第３の実施形態に係るデータ通信装置３における受信可能整数は３７５であり、従来のデータ通信装置９の受信可能整数８１（図１８（ｇ）を参照）よりも大幅に増加している。

【００７１】

以上に説明した通り、第３の実施形態に係るデータ通信装置３によれば、多値符号列１２の各値を累積する累積部１３２１を備えることによって、盗聴者が変調信号１５を受信（傍受）する際に発生する多値識別誤りによる暗号解読防止効果を増大させて受信可能性数を増加させることができる。この結果として、暗号通信における高い安全性を確保できる。また、受信部２０３は、送信部１０３が備える累積部１３２１と同じ構成の累積部２３２１を備えるので、情報データ１０と等しい情報データ２０を復号することが可能となる。

【００７２】

なお、以上では、累積部１３２１は、累積多値符号列１６の（ｋ－１）番目（ｋは自然数）の値を１倍した値に、多値符号列１２のｋ番目の値を加算した値を、累積多値符号列１６のｋ番目の値としている。しかし、累積部１３２１は、累積多値符号列１６の（ｋ－１）番目の値をＰ倍（Ｐは２以上の整数）した値に、多値符号列１２のｋ番目の値を加算した値を、累積多値符号列１６のｋ番目の値としてもよい。詳細については第４の実施形態で説明するが、この様にすることによって、盗聴者が変調信号１４を受信（傍受）する際に発生する多値識別誤りによる暗号解読防止効果を更に増大させることができ、更に受信可能性数を増加させることができる。

【００７３】

また、累積部１３２１は、入力された多値符号列１２の長さが所定長（所定のビット長）に達した場合に、多値符号列１２の累積値である累積多値符号列１６を所定の値（例えば“０”）にリセットしてもよい。ただし、累積部２３２１も同様の動作を行うものとする。このことによって、累積多値符号列１６、２６の値が発散することを防止できる。

【００７４】

また、累積部１３２１は、累積多値符号列１６の値が所定値以上となる度に、累積多値符号列１６を所定の値（例えば“０”）にリセットすることによっても、同様に、当該値の発散を防止できる。ただし、累積部２３２１も同様の動作を行うものとする。

【００７５】

また、累積部１３２１は、累積する多値符号列１２の範囲を、累積時点を基準に、所定長だけ過去の値の範囲までに限定することによっても、累積多値符号列１６の値が発散することを防止できる。具体的には、例えば、累積多値符号列１６の４番目の値は、多値符号列１２の２～４番目の値を用いて生成する。この場合、累積する多値符号列１２の範囲を、累積時点を基準に、２つだけ過去の値の範囲までに限定したこととなる。ただし、累積部２３２１も同様の動作を行うものとする。

【００７６】

また、累積部１３２１は、多値符号列１２の累積値を所定の自然数で割った場合の剰余を累積多値符号列１６として出力することによっても、当該累積値を当該所定の自然数未満に制限して発散を防止できる。ただし、累積部２３２１も同様の動作を行うものとする。

【００７７】

（第４の実施形態）

図１０は、本発明の第４の実施形態に係るデータ通信装置４の構成例を示すブロック図である。図１０に示す通り、データ通信装置４は、データ送信装置１０４（以下、送信部１０４という）とデータ受信装置２０４（以下、受信部２０４という）とが、伝送路１１０を介して接続された構成である。また、データ通信装置４は、第３の実施形態に係るデータ通信装置３（図７を参照）に対して、多値符号変換部１４２、及び多値符号変換部２４２の構成のみが異なる。多値符号変換部１４２は累積部１４２１から構成され、多値符

号変換部２４２は累積部２４２１とから構成される。なお、累積部１４２１と累積部２４２１とは同じ構成であり同じ動作を行うので、累積部２４２１についての説明は省略する。また、以下では、第３の実施形態に係るデータ通信装置３と同じ構成要素については、同じ参照符号を付し、詳しい説明は省略する。

【００７８】

図１１は、図１０に示すデータ通信装置４における受信可能性数を説明するための図である。図１２は、図１１（ｄ）に示す多値信号１４を説明するための図である。なお、以下では、第３の実施形態において説明した内容は省略し、第３の実施形態の内容と異なる部分について詳しく説明する。図１１に示す通り、情報データ１０｛１，０，１，１｝と、多値数ｍ＝８の多値符号列１２｛４，１，４，２｝とが累積部１４２１に入力される場合を一例に挙げて説明する（図１１（ａ）及び（ｂ）を参照）。

【００７９】

累積部１１８は、累積多値符号列１６の（ｋ－１）番目（ｋは、自然数）の値をＰ（Ｐは、２以上の整数）倍した値に、多値符号列１２のｋ番目の値を加算して得られた値を、Ｍ（Ｍは、自然数）で割った剰余を、累積多値符号列１６のｋ番目の値として出力する。ここで、累積多値符号列１６の（ｋ－１）番目の値をαとし、多値符号列１２のｋ番目の値をβとし、累積多値符号列１６のｋ番目の値をγとすると、γ＝ｍｏｄ｛αＰ＋β，Ｍ｝の関係が成り立つ。なお、Ｍは、累積多値符号列１６の多値数となる。

【００８０】

図１１（ｃ）には、具体例として、Ｍ＝８、Ｐ＝２の場合の累積多値符号列１６について記載している。図１１に示す通り、累積多値符号列１６の１番目の値は、累積多値符号列１６の０番目の値“０”（実際には０番目は存在しないので、０番目の値は０と考える）を２倍した値“０”に、多値符号列１２の１番目の値“４”を加算した値“４”を、８で割った剰余“４”となる。同様に、累積多値符号列１６の２番目の値は、累積多値符号列１６の１番目の値“４”を２倍した値“８”に、多値符号列１２の２番目の値“１”を加算した値“９”を、８で割った剰余“１”となる。同様に、累積多値符号列１６の３番目及び４番目の値が出力される。すなわち、累積多値符号列１６として、｛４，１，６，６｝が出力される（図５（ｃ）を参照）。次に、多値処理部１１３は、累積多値符号列１６｛４，１，６，６｝と情報データ１０｛１，０，１，１｝とを入力し、図１６に示す信号フォーマットに従って、多値信号１４｛１２，９，１４，１４｝を生成する（図１１（ｄ）及び図１２を参照）。

【００８１】

次に、盗聴者による盗聴動作について説明する。識別可能数Ｊ＝３と仮定した場合、盗聴者は、盗聴受信部９０３（図１５参照）を用いて伝送路１１０上の変調信号１５を受信して多値識別を行い、受信系列８２として、例えば｛１１，９，１３，１４｝を得ることが可能である（図１１（ｅ）を参照）。そして、盗聴者は、識別可能数Ｊ＝３であることを考慮して、送信された正規の信号である多値信号１４の値が、｛１０～１２，８～１０，１２～１４，１３～１５｝の範囲のいずれかの値であることを推測することが可能である（図１１（ｆ）を参照）。そして、盗聴者は、図１６の信号フォーマットを用いて、送信部１０４で用いられた累積多値符号列１６の値が、｛２～４，０～２，４～６，５～７｝の範囲のいずれかの値であると推測することが可能である（図１１（ｇ）を参照）。

【００８２】

次に、盗聴者は、累積多値符号列１６の推測値｛２～４，０～２，４～６，５～７｝を用いて多値符号列１２を導出するために、送信部１０４が備える累積部１４２１で行われた累積過程を逆算する必要がある。つまり、盗聴者は、上記したγ＝ｍｏｄ｛αＰ＋β，Ｍ｝の関係を用いて、βを算出する必要がある。ここで、多値符号列１２の推測値を｛ｘ１，ｘ２，ｘ３，ｘ４｝と表す。但し、多値符号列１２の多値数ｍは８なので、ｘ１，ｘ２，ｘ３，ｘ４は、０～７の整数のいずれかである。この様に表すと、累積多値符号列１６の１番目の値”２～４”は、累積多値符号列１６の０番目の値“０”を２倍（Ｐ倍）した値“０”に、“ｘ１”を加算した値”ｘ１”を、８で割った剰余となる。つまり、（２

，３，４）＝ｍｏｄ｛０×２＋ｘ１，８｝となる。従って、盗聴者は、ｘ１が“２～４”の範囲のいずれかの値であると推測できる。同様に、累積多値符号列１６の２番目の値”０～２”は、累積多値符号列１６の１番目の値“２～４”を２倍した値“４，６，８”に、それぞれ“ｘ２”を加算した値“４＋ｘ２，６＋ｘ２，８＋ｘ２”を、それぞれ８で割った剰余となる。つまり、（０，１，２）＝ｍｏｄ｛（２，３，４）×２＋ｘ２，８｝となる。従って、盗聴者は、ｘ２が”０～６”の範囲のいずれかの値であると推測できる。以下、同様にして、盗聴者は、ｘ３が”０～６”の範囲のいずれかの値であると推測し、ｘ４が”１～７”の範囲のいずれかの値であると推測できる。この様にして、盗聴者は、多値符号列１２の値が、｛２～４，０～６，０～６，１～７｝の範囲のいずれかの値であると推測できる（図１１（ｈ）を参照）。

【００８３】

このことから、盗聴者は、多値符号列１２が取り得る値を、「３通り×７通り×７通り×７通り＝１０２９通り」の値までしか絞り込むことができない。すなわち、盗聴者が多値符号列１２を解読するために行う処理の試行回数は、計３×７×７×７＝１０２９通りとなる（図１１（ｉ）を参照）。つまり、第４の実施形態に係るデータ通信装置４における受信可能整数は１０２９であり、第３の実施形態において具体的に説明した、データ通信装置３の受信可能整数３７５（図８（ｉ）を参照）を大幅に上まわっている。

【００８４】

以上に説明した通り、第４の実施形態に係るデータ通信装置４によれば、累積多値符号列１８を２倍以上に整数倍する過程を含む累積処理を施す累積部１４２１を備えることによって、盗聴者が変調信号を受信（傍受）する際に発生する多値識別誤りによる暗号解読防止効果を、第３の実施形態において具体的に説明した暗号解読防止効果よりも増大させることができる。この結果として、第４の実施形態に係るデータ通信装置４は、受信可能性数を更に増加させて、暗号通信において更に高い安全性を確保できる。また、第４の実施形態に係るデータ通信装置４は、累積部１４２１が行う上記した累積処理において、既に説明した剰余値を用いて累積多値符号列１６を生成するので、累積多値符号列１６の発散を防止することができる。また、受信部１０４は、累積部１４２１と同じ構成の累積部２４２１を備えるので、情報データ１０と等しい情報データ２０を復号することが可能となる。

【００８５】

なお、累積部１４２１が行う上記した累積処理において用いる２以上の整数Ｐを識別可能数Ｊ以上とすることによって、受信可能整数を最大化することができる。図１３は、識別可能数Ｊ＝Ｐ＝３とした場合の受信可能整数を説明する図である。Ｊ＝Ｐ＝３の条件の下で、盗聴者が、図１１を用いて説明した方法で多値符号列１２を推測すると、多値符号列１２の推測値は、｛２～４，０～７，０～７，０～７｝となる（図１３（ｈ）を参照）。従って、Ｐを識別可能数Ｊ以上とすることによって、受信可能整数を３×８×８×８＝１５３６にまで増加させることができる（図１３（ｉ）を参照）。

【００８６】

ここで、多値符号列１２の推測値の１番目の値は｛２～４｝なので、多値符号列１２の１番目の受信可能性数は３であり、識別可能数Ｊ＝３よりも増加していない。これは、累積多値符号列１６の０番目の値が常に“０”であることによって、多値符号列１２の１番目の値と累積多値符号列１６の１番目の値とが常に等しくなるためである。そこで、累積部１４２１は、累積多値符号列１６の１番目の値を用いずに、累積多値符号列１６の２番目以降の値を用いて多値信号１４を生成する。すなわち、累積多値符号列１６の（ｋ＋１）番目（ｋは自然数）の値を、累積多値符号列１６のｋ番目の値として用いる。このことによって、多値符号列１２の１番目の値の受信可能性数を、２番目以降の受信可能性数８と等しくすることができる。この結果として、受信可能整数は、８×８×８×８＝４０９６にまで増加する。そして、多値符号列１２の多値数ｍは８なので、盗聴者は多値符号列１２の値を絞り込むことができなくなる。

【００８７】

この様に、Ｐを識別可能数Ｊ以上にし、累積多値符号列１６の２番目以降の値を用いて多値信号１４の生成することによって、盗聴者が解読時に考慮しなければならない、多値符号列１２の各値の受信可能性数は、最大で識別可能数Ｊの２乗まで増加する。従って、累積多値符号列１６の多値数Ｍを識別可能数Ｊの２乗以下に設定することによって、多値符号列１２の各値の受信可能性数は多値数Ｍまで増加して、暗号解読に要する計算量を最大にできる。

【００８８】

（第５の実施形態）

図１４は、本発明の第５の実施形態に係るデータ送信装置５の構成例を示すブロック図である。図１４に示す通り、データ通信装置５は、データ送信装置１０５（以下、送信部１０５という）と、データ受信装置２０５（以下、受信部２０５という）とが、伝送路１１０を介して接続された構成である。送信部１０５は、２値乱数発生部１５１と、多値符号変換部１５２と、多値化部１５５と、多値処理部１１３と、変調部１１４とを備える。受信部２０５は、復調部２１３と、識別部２１４と、２値乱数発生部２５１と、多値符号化部２５２と、多値化部２５５とを備える。ただし、多値符号変換部１５２は累積部１５２１から構成され、多値符号変換部２５２は累積部２５２１をから構成される。なお、以下では、第３の実施形態に係るデータ通信装置３と同じ構成要素については、同じ参照符号を付し、詳しい説明は省略する。

【００８９】

送信部１０５において、２値乱数発生部１５１は、鍵情報１１に基づいて、略乱数的に２値に値が変化する２値乱数列１７を生成する。２値乱数列１７は、多値変換部１５２に入力される。多値変換部１５２において、累積部１５２１は、２値乱数列１７をｒビット（ｒは、自然数）のブロックに分割し、当該分割したブロックの内の２つ以上のブロックを累積した累積２値乱数列１８を生成する。多値化部１５５は、所定の多値符号化則（例えば、図１６に示す信号フォーマット）に従って、累積２値乱数列１８を略乱数的に値が変化する多値符号列１２に変換する。これ以降の動作は、第３及び第４の実施形態に記載した動作と同様であるので省略する。そして、受信部２０５において、２値乱数発生部２５１が送信側の２値乱数発生部１５１と同じ動作をし、累積部２５２１が送信側の累積部１５２１と同じ動作をし、多値化部２５５が送信側の多値化部１５５と同じ動作をする。このことによって、受信部２０５は、情報データ１０と等しい情報データ２０を復号することができる。

【００９０】

以上に説明した通り、第５の実施形態に係るデータ通信装置５によれば、２値乱数列に対して累積処理を施して得られる累積２値乱数列を多値化して多値符号列を得ることができる。これによって、第３の実施形態に係るデータ通信装置３と同様に受信可能性数を増加させて暗号通信における高い安全性を確保できる。

【００９１】

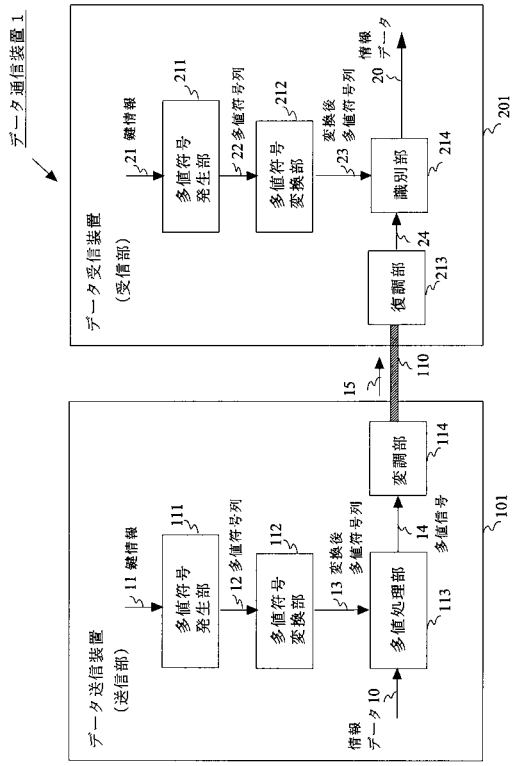
なお、第５の実施形態に係るデータ通信装置５においても、第３の実施形態に係るデータ通信装置３及び第４の実施形態に係るデータ通信装置４と同様に、累積２値乱数列の発散を防止することができる。具体的には、累積部１５２１は、入力された２値符号列１７の長さが所定長（所定の符号数）に達した場合に、２値符号列１７の累積値である累積２値符号列１８の値を所定の値をリセットし、累積部２５２１も同様の動作を行う。このことによって、累積２値符号列１８、２８の値が発散することを防止できる。同様に、第３の実施形態及び第４の実施形態で説明した、発散を防止する他の方法についても、データ通信装置５に用いることができる。

【００９２】

また、上述した第１～第５の実施形態についての説明では、図１６に示す信号フォーマットを用いる場合について説明したが、使用する信号フォーマットはこれには限られず、例えば、変調ペアの高い方のレベルに情報データ“１”が常に割当てられ、低い方のレベルに情報データ“０”が常に割当てられる信号フォーマットを使用してもよい。

【００９３】
以上、本発明を詳細に説明してきたが、前述の説明はあらゆる点において本発明の例示にすぎず、その範囲を限定しようとするものではない。本発明の範囲を逸脱することなく種々の改良や変形を行うことができることは言うまでもない。
【産業上の利用可能性】
【００９４】
本発明に係るデータ通信装置は、盗聴・傍受等を受けない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】
【００９５】
【図１】本発明の第１の実施形態に係るデータ通信装置１の構成例を示すブロック図
【図２Ａ】非可逆な変換処理による変換後多値符号列１３の生成過程の一例を示す図
【図２Ｂ】盗聴者による変換後多値符号列１３の解読処理を説明する図
【図３Ａ】複数シンボル毎に変換後多値符号列１３を生成する過程を説明する図
【図３Ｂ】盗聴者による複数シンボル毎に生成された変換後多値符号列１３の解読処理を説明する図
【図４】本発明の第２の実施形態に係るデータ通信装置２の構成例を示すブロック図
【図５】本発明の第２の実施形態に係るデータ通信装置２ａの構成例を示すブロック図
【図６】多値符号発生部１１１の構成の一例を示すブロック図
【図７】本発明の第３の実施形態に係るデータ通信装置３の構成例を示すブロック図
【図８】図７に示すデータ通信装置３における受信可能性数を説明するための図
【図９】図８（ｃ）に示す多値信号１４を説明するための図
【図１０】本発明の第４の実施形態に係るデータ通信装置４の構成例を示すブロック図
【図１１】図１０に示すデータ通信装置４における受信可能性数を説明するための図
【図１２】図１１（ｄ）に示す多値信号１４を説明するための図
【図１３】識別可能数Ｊ＝Ｐ＝３とした場合の受信可能整数を説明するための図
【図１４】本発明の第５の実施形態に係るデータ送信装置５の構成例を示すブロック図
【図１５】Ｙ－００プロトコルを用いた従来のデータ通信装置９の構成例を示すブロック図
【図１６】Ｙ－００プロトコルを用いた従来のデータ通信装置９が用いる多値信号の信号フォーマットを示す図
【図１７】従来のデータ通信装置９の動作について具体的に説明するための図
【図１８】図１５に示す従来のデータ通信装置９における受信可能性数を説明するための図
【図１９】図１８（ｃ）に示す多値信号９３を説明するための図
【符号の説明】
【００９６】
１～５　データ通信装置
１１１，２１１　多値符号発生部
１１１ｘ　２値乱数発生部
１１１ｙ　多値化部
１１２，２１２，１３２，２３２　多値符号変換部
１３２１，２３２１　累積部
１１３　多値処理部
１１４　変調部
２１３　復調部
２１４　識別部

【図１】



【図２Ａ】

多値符号列12	0	1	2	3	4	5	6
3を減算した 多値符号列12	-3	-2	-1	0	1	2	3
変換後 多値符号列13	3	2	1	0	1	2	3

変換処理

【図２Ｂ】

変換後 多値符号列13	3	2	1	0	1	2	3
盗聴者が想定する 多値符号列12の候補	0 or 6	1 or 5	2 or 4	3	2 or 4	1 or 5	0 or 6
数理アルゴリズムを 適用する組み合わせ数	2 × 2 × 2 × 1 × 2 × 2 × 2 = 64通り						

包含

【図３Ａ】

多値符号列12	6	3	7	2	5	1
変換後 多値符号列13	9		9		6	

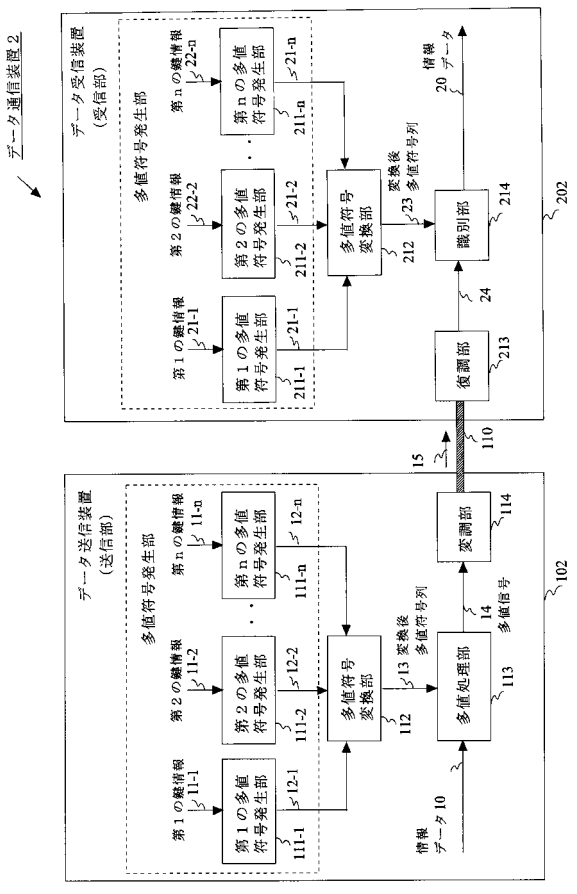
変換処理
(加算)

【図３Ｂ】

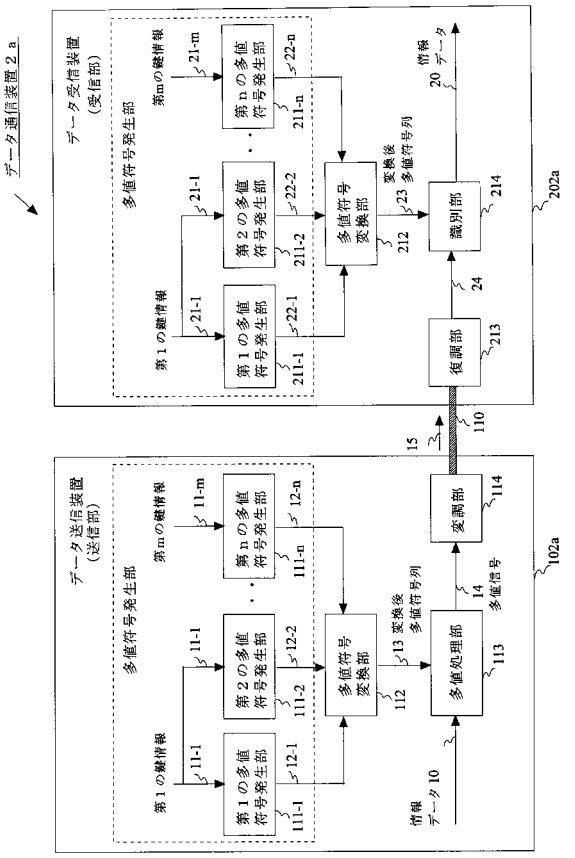
変換後 多値符号列13	9	9	6
盗聴者が 想定する 多値符号列12の候補	(2, 7) (3, 6) (4, 5) (5, 4) (6, 3) (7, 2)	(2, 7) (3, 6) (4, 5) (5, 4) (6, 3) (7, 2)	(0, 6) (1, 5) (2, 4) (3, 3) (4, 2) (5, 1) (6, 0)
数理アルゴリズムを 適用する組み合わせ数	6 × 6 × 7 =252通り		

包含

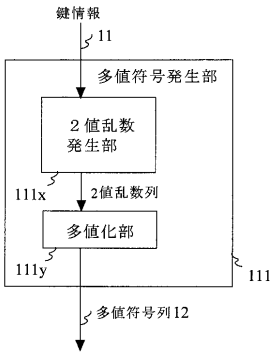
【図４】



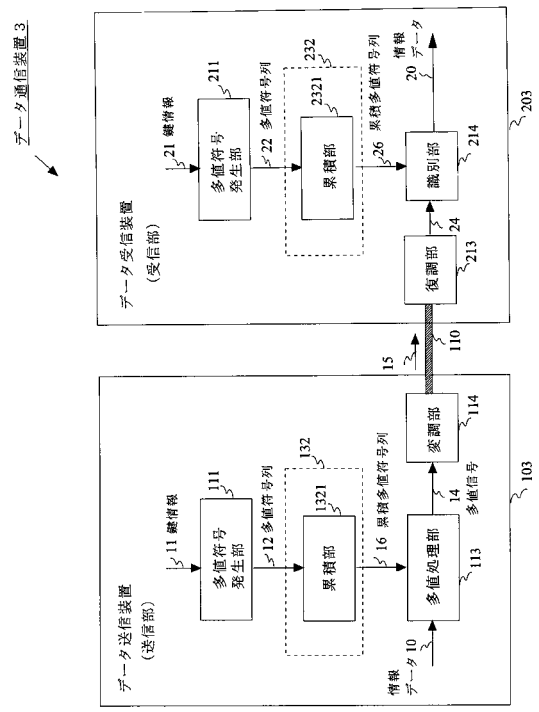
【図５】



【図６】



【図７】



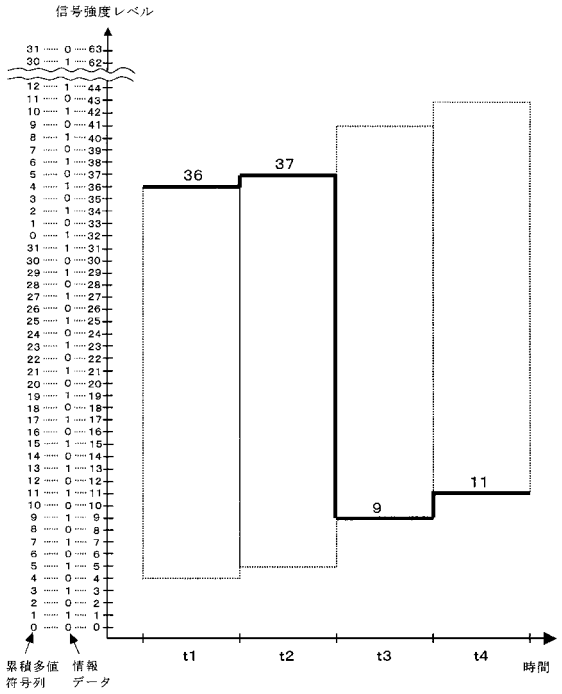
【図８】

（ａ）情報データ10	1	0	1	1	
（ｂ）多値符号列12	4	1	4	2	(m=8)
（ｃ）累積多値符号列16	4	5	9	11	(m=32)
（ｄ）多値信号14	36	37	9	11	
伝送					
（ｅ）盗聴者の受信系列82	35	38	9	11	(識別可能数J=3)
（ｆ）送信された多値信号14の推定値	34～36	37～39	8～10	10～12	
（ｇ）送信時に用いられた累積多値符号列16の推定値	2～4	5～7	8～10	10～12	
	(x1)	(x2)	(x3)	(x4)	
（ｈ）送信時に用いられた多値符号列12の推定値	2～4	1～5	1～5	0～4	

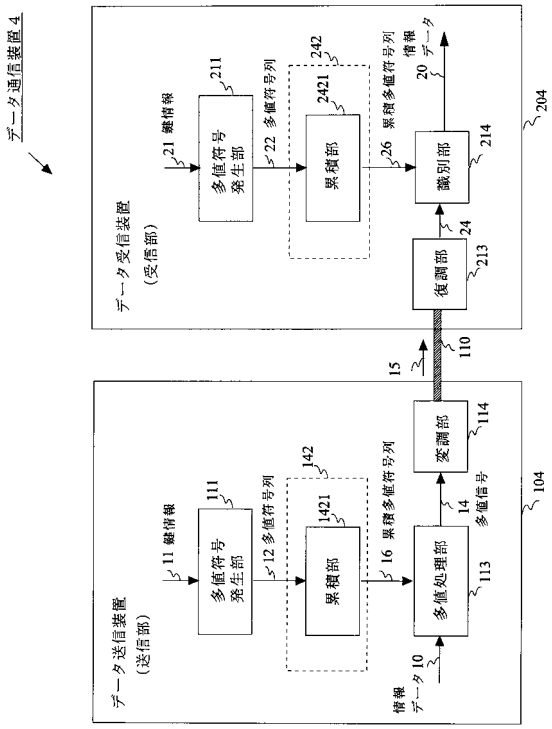
{(2, 3, 4)+x2}=5, 6, 7 但し、x2は0～(m-1) {2+x2}=5, 6, 7→x2=3, 4, 5 {3+x2}=5, 6, 7→x2=2, 3, 4 {4+x2}=5, 6, 7→x2=1, 2, 3	{(5, 6, 7)+x3}=8, 9, 10 但し、x3は0～(m-1) {5+x3}=8, 9, 10→x3=3, 4, 5 {6+x3}=8, 9, 10→x3=2, 3, 4 {7+x3}=8, 9, 10→x3=1, 2, 3	{(8, 9, 10)+x4}=10, 11, 12 但し、x4は0～(m-1) {8-x4}=10, 11, 12→x4=2, 3, 4 {9+x4}=10, 11, 12→x4=1, 2, 3 {10+x4}=10, 11, 12→x4=0, 1, 2

（ｉ）受信可能性数 ＝ 3 × 5 × 5 × 5 ＝ 375

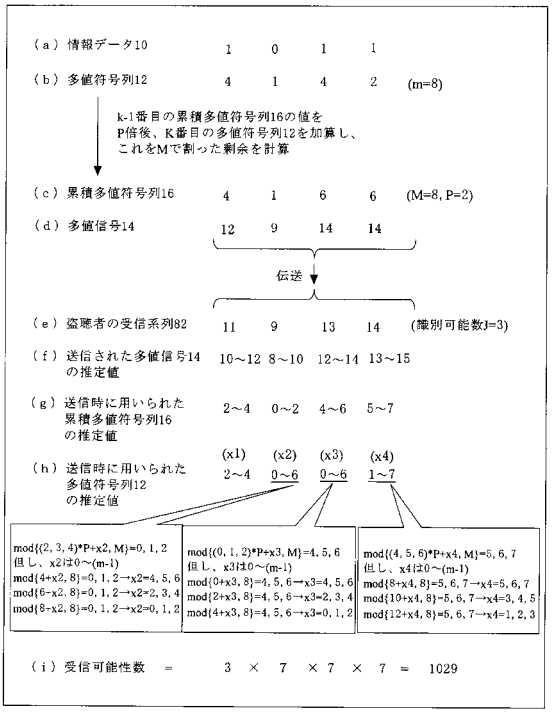
【図９】



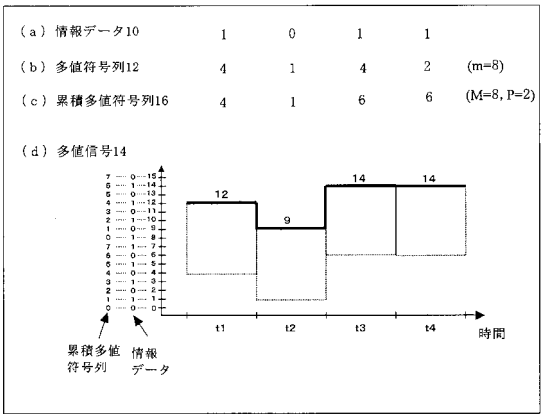
【図１０】



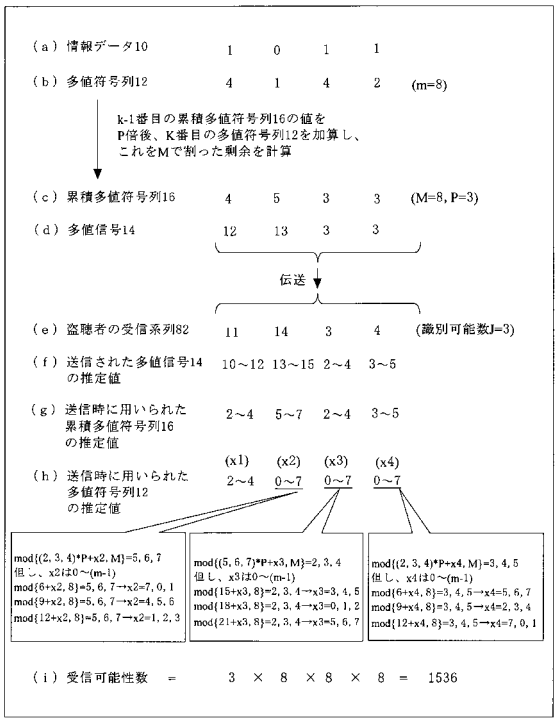
【図１１】



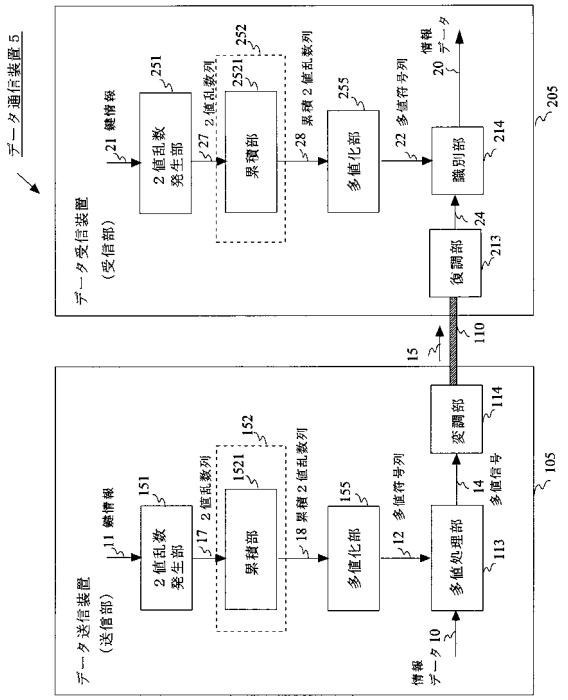
【図１２】



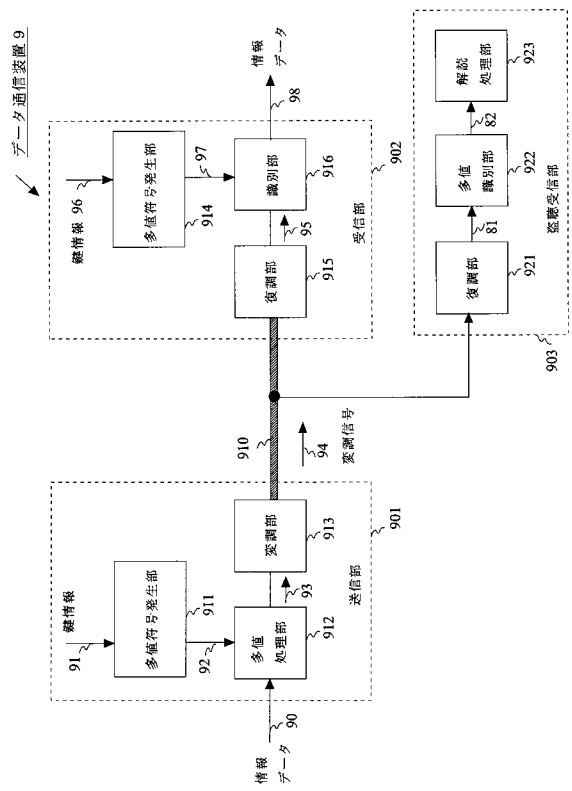
【図１３】



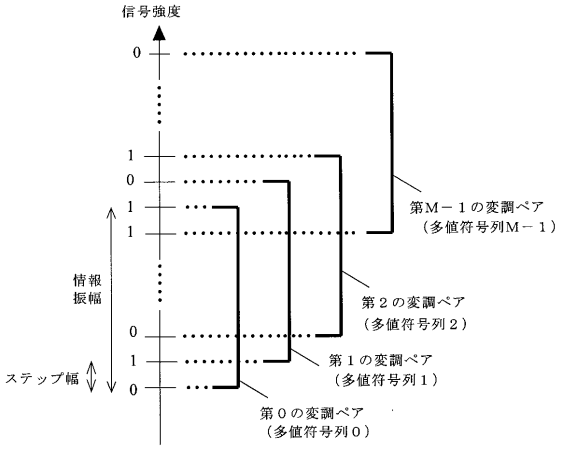
【図１４】



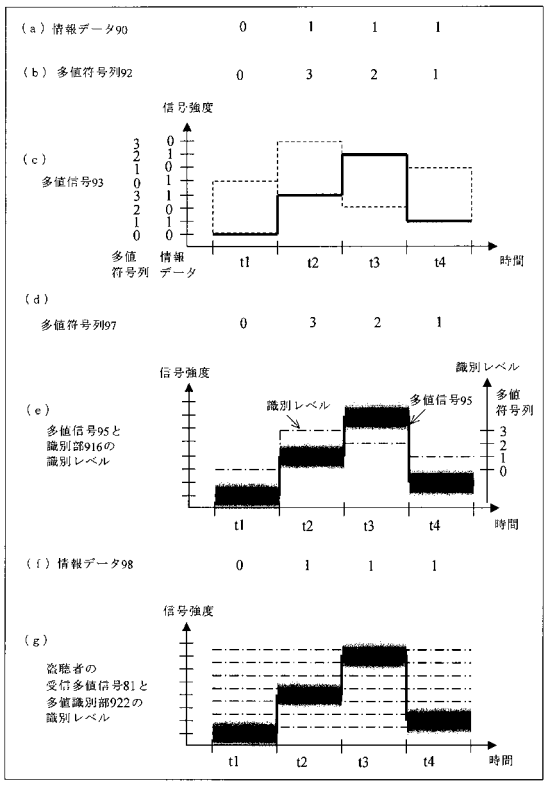
【図１５】



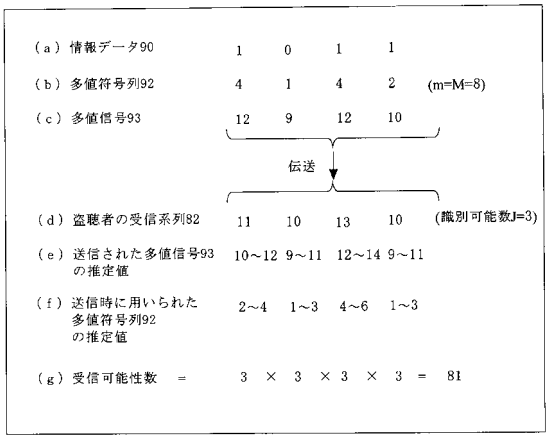
【図１６】



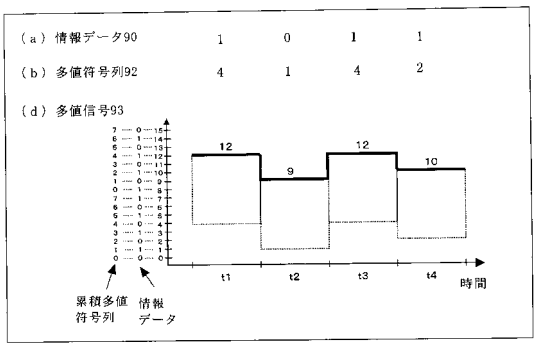
【図１７】


（ａ）情報データ90
0 1 1 1
（ｂ）多値符号列92
0 3 2 1
信号強度
（ｃ）
多値信号93
多値符号列
情報データ
t1 t2 t3 t4
時間
（ｄ）
多値符号列97
0 3 2 1
信号強度
識別レベル
（ｅ）
多値信号95と識別部916の識別レベル
識別レベル
多値信号95
多値符号列
t1 t2 t3 t4
時間
（ｆ）情報データ98
0 1 1 1
信号強度
（ｇ）
盗聴者の受信多値信号81と多値識別部922の識別レベル
t1 t2 t3 t4
時間

【図１８】


（ａ）情報データ90 1 0 1 1
（ｂ）多値符号列92 4 1 4 2 (m=M=8)
（ｃ）多値信号93 12 9 12 10
伝送
（ｄ）盗聴者の受信系列82 11 10 13 10 (識別可能数J=3)
（ｅ）送信された多値信号93の推定値 10～12 9～11 12～14 9～11
（ｆ）送信時に用いられた多値符号列92の推定値 2～4 1～3 4～6 1～3
（ｇ）受信可能性数 = 3 × 3 × 3 × 3 = 81

【図１９】


（ａ）情報データ90 1 0 1 1
（ｂ）多値符号列92 4 1 4 2
（ｄ）多値信号93
12
9
12
10
t1 t2 t3 t4
時間
累積多値符号列
情報データ

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
(72)発明者　大平　智亮
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　松平　英

(56)参考文献　国際公開第２００６／０２５４２６（WO，Ａ１）
特開２００６－１５７６３９（ＪＰ，Ａ）
特開２００６－３０３９２７（ＪＰ，Ａ）
特開２００７－２７４３００（ＪＰ，Ａ）
特開２００８－２４５０５３（ＪＰ，Ａ）
国際公開第２００６／０３８６６０（WO，Ａ１）
国際公開第２００７／０４３２９７（WO，Ａ１）
特開平０５－１６５４７０（ＪＰ，Ａ）
特開２００４－３４８４６０（ＪＰ，Ａ）
林　正樹，４．基本的なディジタルビデオ回路，エレクトロニクスライフ，日本放送出版協会，１９９３年　5月　1日，第７２９号，ｐ．５１～６１
生島　剛　他，量子ゆらぎ拡散暗号伝送方式（Ｙ－００）の開発（１）－１Ｇｂｐｓ光伝送装置－，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，社団法人電子情報通信学会，２００５年　9月　7日，ｐ．３００
小林　洋平　他，光通信量子暗号（Ｙ－００）における量子ゆらぎエラーの均一化，電子情報通信学会２００６年総合大会講演論文集　通信２，社団法人電子情報通信学会，２００６年　3月　8日，ｐ．３５８
佐田　友和　他，量子ゆらぎ拡散伝送における多値符号化方式の検討，電子情報通信学会２００６年通信ソサイエティ大会講演論文集２，社団法人電子情報通信学会，２００６年　9月　7日，ｐ．２１１
佐田　友和　他，量子ゆらぎ拡散伝送信号の盗聴誤りが鍵絞込み効率に及ぼす影響，電子情報通信学会２００７年総合大会講演論文集　通信２，社団法人電子情報通信学会，２００７年　3月　7日，ｐ．４１７

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｋ　　１／００
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２４
Ｈ０４Ｎ　　７／１６７