世界知的所有権機関
国際事務局

PCT

特許協力条約に基づく国際出願

(51) 国際特許分類6		(11) 国際公開番号	WO96/02992
H04L 9/28	A1	(43) 国際公開日	1996年2月1日(01.02.96)

(21) 国際出願番号 PCT/JP95/01410
(22) 国際出願日 1995年7月14日(14.07.95)

(30) 優先権データ
特願平6/164103 1994年7月15日(15.07.94) JP

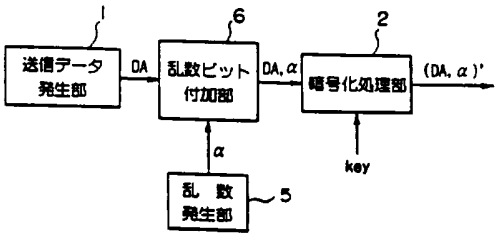
(71) 出願人（米国を除くすべての指定国について）
エヌ・ティ・ティ移動通信網株式会社
(NTT MOBILE COMMUNICATIONS NETWORK INC.)[JP/JP]
〒105 東京都港区虎ノ門二丁目10番1号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
前原昭宏(MAEBARA, Akihiro)[JP/JP]
〒235 神奈川県横浜市磯子区杉田9-2-12
富岡第一寮A-312 Kanagawa, (JP)
小林勝美(KOBAYASHI, Katsumi)[JP/JP]
〒233 神奈川県横浜市港南区日限山3-42-5-103 Kanagawa, (JP)
岡島一郎(OKAJIMA, Ichiro)[JP/JP]
〒235 神奈川県横浜市磯子区森6-18-3-305 Kanagawa, (JP)
内田慎子(UCHIDA, Noriko)[JP/JP]
〒231 神奈川県横浜市中区根岸町2-110-703 Kanagawa, (JP)
上林真司(UEBAYASHI, Shinji)[JP/JP]
〒231 神奈川県横浜市金沢区能見台4-4-21 D-301
Kanagawa, (JP)
(74) 代理人
弁理士 川崎研二, 外(KAWASAKI, Kenji et al.)
〒104 東京都中央区京橋一丁目4番11号
竹本ビル2F Tokyo, (JP)

(81) 指定国
JP, US, 欧州特許(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類 国際調査報告書

(54) Title : SIGNAL TRANSMITTING METHOD AND COMMUNICATION SYSTEM

(54) 発明の名称 信号伝送方式および通信システム



1 ... transmission data generator
2 ... enciphering section
5 ... random number generator
6 ... random number bit adding section

(57) Abstract

Signals are transmitted in secret even when the information representing the destination terminal is opened because a common access channel is used. Obstruction can be well prevented. A random number bit adding section (6) adds a random number α (digital signal) generated by a random number generator (5) to the transmission data DA generated by a transmission data generator (1), and outputs the composite signal (DA, α). An enciphering section (2) enciphers the signal (DA, α) and outputs the ciphered signal (DA, α)'. A receiving device deciphers the ciphered signals (DA, α)' to the original signals (DA, α) and reproduces the data DA by removing the random number bit α.

（５７）要約

共通アクセスチャンネルを用いるために相手端末を示す情報がオープンになる場合でも、伝送信号自体を良好に秘匿し、妨害を十分に押さえる。

乱数ビット付加部６においては、送信データ発生部１が発生する送信データＤＡに、乱数発生部５が発生した乱数α（デジタル信号）が付加され、信号（ＤＡ，α）として出力される。そして、暗号化処理部２は、信号（ＤＡ，α）を暗号化し、信号（ＤＡ，α）’として出力する。この信号（ＤＡ，α）’は受信装置において解読されて（ＤＡ，α）に戻り、さらに、乱数ビットαが除去されて信号ＤＡが復元される。

明 細 書

信号伝送方式および通信システム

技 術 分 野

この発明は、例えば、共通アクセスチャンネルに複数の移動局がアクセスする場合に用いて好適な信号伝送方式および通信システムに関する。

技 術 背 景

共通のチャンネルに複数の端末がアクセスするようなデジタル信号伝送の場合は、自局や通信相手を示す識別情報が必要になる。なぜならば、共通チャンネルには任意の端末がアクセスするため、どの端末からどの端末に向けての信号であるかが不明であると、信号伝送そのものが不能になってしまうからである。このような状況は、移動電話においてパケット通信を行う場合も同様である。

ところで、上述のような環境においては、どの端末がどの端末に信号を伝送しているのかがオープンになっているため、相手の端末（あるいは移動局）を示す識別情報が容易に傍受できる。このため、悪意に妨害を行おうとすれば、簡単に行うことができ、例えば、傍受した相手先に何らかの信号を転送して妨害することなどが容易に行える。

そこで、妨害防止のため、信号を秘匿化することが考えられるが、相手先については通信システムの都合上どうしても秘匿化できないため、伝送信号についてのみ秘匿化しなければならないという事情がある。

ここで、信号を暗号化する構成例を図１６に示す。図１６において、１は送信すべきデータを発生する送信データ発生部であり、ここで作成されたデータＤＡは、暗号化処理部２において所定のアルゴリズムに基づいて暗号化される。この暗号化に際しては、鍵Ｋｅｙが用いられ、したがって、このように暗号化された信号を受信するときは、送信側が用いた鍵Ｋｅｙと同じものを用いて暗号解読すればよい。この場合、送信側と受信側とは非同期であるため、鍵Ｋｅｙを適宜変更することはできず、所定の固定鍵が用いられる。

ところで、図１６に示す構成においては、一応信号の秘匿化ができるが、送信

データが単純な場合は、暗号化された結果を見ただけでも、元のデータが推定できることがあり、妨害防止の観点からは十分な秘匿性があるとは言えない。

例えば、移動通信の制御信号などは、データが限られていて種類が少なく、例えば、3種類程度の場合もある。一方、固定鍵を用いて同じアルゴリズムで暗号化を行えば、暗号化された信号の種類も元の信号と同じ数になるから、容易に原信号が明らかになってしまう。すなわち、信号を同一鍵を用いて暗号化する方式では、信号のパターンの種類が少ない場合、暗号化の結果のパターンも少なくなり、原信号を容易に類推できてしまう。

このため、システムに精通している悪意の第3者が信号をモニタした場合、暗号化の結果であるパターンの発生頻度や信号長などのモニタ結果から得られる情報により、送受信された信号が「何の信号」かを推定できる可能性が高い。特に、制御信号の場合には、接続や切断など、何のための制御信号かが推定できてしまう。

このようにして、何の信号かが判ると、上記第3者は秘匿の鍵を知らなくても、正当な端末が発生する信号と同一の信号を発生することができるため、正当な端末になりすまして、通信を妨害することが可能になる。

例えば、移動電話によるパケット通信などのように、制御信号の種類が少ない場合などは、上述の事情から、単なる暗号化だけでは妨害の対策にならないことがある。しかも、モニタされ易い通信環境であるため、その対策が望まれていた。

発明の開示

この発明は、上述した事情に鑑みてなされたもので、共通アクセスチャンネルを用いるために相手端末を示す情報がオープンになる場合でも、伝送信号自体を良好に秘匿し、妨害を十分に押さえることができる信号伝送方式および通信システムを提供することを目的としている。

上記課題を解決するために、請求項1記載の発明においては、送信側は、伝送すべき信号の所定位置に乱数のビットを付加するとともに、所定の鍵を用いて暗号化して送信し、受信側は、受信信号を前記所定の鍵を用いて暗号解読するとともに、解読後の信号の所定位置から前記乱数のビットを除去することを特徴とす

る。

また、請求項２に記載の発明においては、送信側は、伝送すべき信号の所定位置に乱数のビットおよび自局を識別する識別情報のビットを付加するとともに所定の鍵を用いて暗号化して送信し、受信側は、受信信号を前記所定の鍵を用いて暗号解読するとともに、解読後の信号の所定位置から前記乱数のビットを除去し、かつ、前記識別情報が送信側の装置の識別情報と一致するか否かを判定し、一致する場合に正常受信したと判断することを特徴とする。

また、請求項３に記載の発明においては、送信装置は、所定ビットの乱数を発生する乱数発生手段と、送信すべき信号を送出する送信信号発生手段と、前記送信信号発生手段が出力する信号の所定位置に前記乱数発生手段が発生した乱数のビットを付加して出力する乱数付加手段と、前記乱数付加手段の出力信号を所定の鍵を用いて暗号化する暗号化手段とを具備し、受信装置は、前記所定の鍵を用いて受信信号の暗号を解いて出力する暗号解読手段と、前記暗号解読手段の出力信号の所定位置から乱数のビットを除去して出力する乱数ビット除去手段とを具備することを特徴とする。

また、請求項４に記載の発明においては、送信装置は、所定ビットの乱数を発生する乱数発生手段と、伝送すべき信号を送出する送信信号発生手段と、前記送信信号発生手段が出力する信号の所定位置に前記乱数発生手段が発生した乱数のビットおよび自装置を識別するための識別情報のビットを付加して出力するビット付加手段と、前記ビット付加手段の出力信号を所定の鍵を用いて暗号化する暗号化手段と、を具備し、受信装置は、前記所定の鍵を用いて受信信号の暗号を解いて出力する暗号解読手段と、前記暗号解読手段の出力信号の所定位置から乱数のビットを除去する乱数ビット除去手段と、前記暗号解読手段の出力信号に含まれる識別情報が前記送信装置の識別情報と一致するか否かを判定し、一致していた場合に当該受信信号を有効と判定する判定手段とを具備することを特徴とする。

請求項５に記載の発明においては、送信側は、乱数のビットを付加する位置を示す乱数位置情報を発生し、この乱数位置情報に応じたビット位置に乱数を付加し、受信側は、送信側と同じ値の乱数位置情報を送信側と同じ順序で発生し、乱数ビットを除去する際には、発生した乱数位置情報に対応するビット位置から乱

数を除去することを特徴とする。

請求項６に記載の発明においては、前記送信装置は、乱数のビットを付加する位置を示す乱数位置情報を発生する第１の乱数位置情報発生手段を有し、前記乱数付加手段は前記第１の乱数位置情報発生手段が発生した乱数位置情報に応じた位置に前記乱数を付加し、前記受信装置は、前記第１の乱数位置情報発生手段が発生する位置情報と同じ値の位置情報を同じ順序で発生する第２の乱数位置情報発生手段を有し、前記乱数ビット除去手段は前記第２の乱数位置情報発生手段が発生した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする。

請求項７に記載の発明においては、前記送信側は、乱数のビットを付加する位置を示す乱数位置情報を発生し、この乱数位置情報に応じたビット位置に乱数を付加するとともに、前記送信信号に前記乱数位置情報を付加し、前記受信側は、受信信号から乱数位置情報を抽出し、乱数ビットを除去する際には、抽出した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする。

請求項８に記載の発明においては、前記送信装置は、乱数のビットを付加する位置を示す乱数位置情報を発生する乱数位置情報発生手段と、前記乱数位置情報を前記送信信号に付加する乱数位置信号付加手段とを有し、前記乱数付加手段は前記乱数位置情報発生手段が発生した乱数位置情報に応じた位置に前記乱数を付加し、前記受信装置は、前記受信信号から乱数位置情報を抽出する乱数位置情報抽出手段を有し、前記乱数ビット除去手段は前記乱数位置情報抽出手段が抽出した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする。

請求項９に記載の発明においては、前記送信側は、次に送信すべき送信信号の乱数位置情報を、その直前に送信する送信信号に付加し、前記受信側は、直前の受信信号から抽出した乱数位置情報に基づいて次の受信信号から乱数を除去することを特徴とする。

請求項１０に記載の発明においては、前記送信装置の乱数付加手段は、次に送信すべき送信信号の乱数位置情報を、その直前に送信する送信信号に付加し、前記受信装置の乱数ビット除去手段は、前記乱数位置情報抽出手段が直前の受信信号から抽出した乱数位置情報に基づいて次の受信信号から乱数を除去することを

特徴とする。

（作用）

請求項１、３に記載の発明では、以上のように構成したので、伝送すべき信号の所定位置に乱数ビットが付加され、これが所定の鍵を用いて暗号化されるから、暗号化された信号をそのまま解読しても元の信号は復元できない。一方、解読した信号の所定位置から乱数ビットを除去すれば、元の信号が復元される。

この場合、乱数を付与して暗号化するので、１つの信号に対して複数の暗号化結果が得られるので、上述の弊害を防止することができる。すなわち、第３者にとっては、妨害が極めて難しいが、送信側と受信側においては、簡単な処理によって情報の秘匿化が行える。この場合、伝送信号に付加されるアドレスは秘匿化しないが、これが傍受されても第３者は信号部分についての復元ができないから、妨害を未然に防止することができる。

請求項２、４に記載の発明においては、以上のように構成したので、送信側で装置を識別するための識別情報を併せて暗号化し、これを受信側において復元すれば、受信信号内の識別情報と送信装置の識別情報との一致を判定することができ、この一致により、受信信号の正否を決めることができる。例えば、秘匿の鍵は固定長であるため、鍵のパターンも限られているため（一例として、秘匿の鍵が８バイトの場合には鍵のパターンは2^{64}通りになる）、同一時間帯に同一の鍵を用いて通信を行う端末が存在する可能性がある。そこで、端末を識別する識別情報を付与することにより、同一鍵を使用している端末からの信号を誤って受信してしまうことを防止することができる。

請求項５、６に記載の発明では、以上のように構成したので、乱数が付与される位置をランダムに変化させることができ、さらに、受信側においては、送信側と同じ乱数付与位置の情報を持つことにより、信号の復元を良好に行うことができる。また、乱数の位置を変化させることにより、信号を暗号化した際に発生するパターンを変化させることができるため、少ない種類の乱数で多数のパターンを発生することができる。このため、乱数ビット数が請求項１、３に記載の発明と同じであっても、発生するパターン数を大幅に増加させることができ、これにより、信号内容を推定するのは極めて困難になる。また、逆に発生するパターン

数を請求項１、３に記載の発明と同じにする場合は、乱数ビット数は少なくて済むため、少ない情報量で同一の効果を得ることができる。

請求項７、８に記載の発明では、上述のように構成したので、受信信号に含まれる乱数位置情報に基づいて、乱数の位置を知ることができる。一方、請求項５、６に記載の発明は、乱数の付与位置情報を送受信側双方で予め固定的に持ち、受信信号からは乱数位置を知ることができないため、信号消滅時などにおいては送信側と受信側とで乱数付与位置に対する不一致が起こり、それ以降の信号が受信できないという危険がある。これに対し、請求項７、８に記載の発明では、乱数の付与位置情報を送信信号に含ませることにより、信号が消滅した場合でも、次の信号を正常に受信することができる。

請求項９、１０に記載の発明では、上述のように構成したので、送信側では、次の信号に対応する乱数位置情報を、前の信号に付加して送信し、また、受信側では一つ前の信号に付加されていた乱数位置情報を用いて新たな受信信号から乱数を除去する。このように、乱数の付与位置情報を送信信号に含ませることにより、請求項７、８に記載の発明と同様に効果を得ることができる。

図面の簡単な説明

図１は、この発明の第１実施例における送信装置の構成を示すブロック図である。

図２は、同実施例の受信装置の構成を示すブロック図である。

図３は、乱数ビット付加部６の出力信号のデータ構造を示す図である。

図４は、乱数ビット付加部６の出力信号の他のデータ構造を示す図である。

図５は、乱数ビット付加部６の出力信号の他のデータ構造を示す図である。

図６は、同実施例の変形例における送信装置の構成を示すブロック図である。

図７は、同実施例の変形例における受信装置の構成を示すブロック図である。

図８は、ビット付加手段９の出力信号のデータ構造を示す図である。

図９は、この発明の第２実施例の送信装置の構成を示すブロック図である。

図１０は、同実施例の受信装置の構成を示すブロック図である。

図１１は、乱数位置情報ＲＰの機能を説明するための図である。

図１２は、この発明の第３実施例の送信装置の構成を示すブロック図である。

図１３は、同実施例の受信装置の構成を示すブロック図である。

図１４は、乱数ビット付加部の構成例を示すブロック図である。

図１５は、乱数ビット除去部の構成例を示すブロック図である。

図１６は、送信データを暗号化する場合の一般的な構成例を示すブロック図である。

発明を実施するための最良の形態

Ａ－１：第１実施例の構成

この発明の第１実施例における送信装置について図１を参照して説明する。この図に示す１は送信すべき信号を発生する送信データ発生部、２は暗号化を行う暗号化処理部であり、各々図１６で示したものと同様である。また、５は乱数を発生する乱数発生部であり、発生した乱数α（デジタル信号）は乱数ビット付加部６において信号ＤＡに付加される。この場合、乱数αは、予め定められたビット数で発生される。

また、乱数ビット付加部６においては、図３に示すように、信号ＤＡに対して乱数αのビットが付加され、信号（ＤＡ，α）として出力される。そして、暗号化処理部２においては、信号（ＤＡ，α）を暗号化し、信号（ＤＡ，α）’として出力する。

一方、図２はこの実施例の受信装置の構成を示すブロック図であり、図において１０は伝送されてきた信号（ＤＡ，α）’を所定の鍵Ｋｅｙを用いて解読する解読処理部であり、解読の結果として信号（ＤＡ，α）を出力する。次に、暗号ビット除去部１１は、信号（ＤＡ，α）から乱数ビットαを除去し、信号ＤＡだけにして後段の回路に伝達する。

Ａ－２：第１実施例の動作

上述した構成によれば、送信装置が出力する信号は、信号ＤＡに乱数αのビットが付加されたものを暗号化した信号になるので、信号ＤＡの種類が少い場合でも、送信装置が出力する信号の種類は乱数のビットに応じて飛躍的に増大する。

この場合、暗号化のアルゴリズム、およびその鍵Ｋｅｙは変化しなくても、暗

号化された信号は乱数αに応じて多様に変化したものとなるから、（ＤＡ，α）’から信号ＤＡを推定することはできない。したがって、信号の秘匿性はきわめて高いものとなる。

一方、受信装置においては、信号解読処理部１０において、固定の鍵Ｋｅｙを用いて信号（ＤＡ，α）’を解読し、その後に乱数ビット除去部１１において乱数ビットを除去すれば容易に信号ＤＡを再現することができる。

上述の処理においては、送信装置と受信装置との間において、暗号化のアルゴリズム、鍵Ｋｅｙ、乱数αのビット数、および乱数ビットの挿入位置について予め決めておけば、送信装置が発生する信号ＤＡは受信装置において確実に再現される。

なお、図３に示す例においては、信号ＤＡの後に乱数αのビットが付加されたが、乱数の付加位置はこれに限らず、信号ＤＡの開始部分でもよく、また、図４に示すように信号ＤＡの途中に挿入してもよい。要は、挿入されるビット位置が判っていれば、受信装置側では容易に信号ＤＡが再現される。

さらに、図５に示すように、乱数のビットをα_1、α_2に分割し、これを信号ＤＡに付加するようにしてもよい。

Ａ－３：第１実施例の変形

次に、上述した実施例の変形例について図６～図８を参照して説明する。この変形例においては、まず、図６に示すように、識別情報発生部８において、当該装置を識別するための識別情報ＩＤを発生するとともに、ビット付加手段９において、この識別情報ＩＤと乱数αとを信号ＤＡに加算する（図８参照）。この結果、暗号化処理部２から出力される信号は（ＤＡ，ＩＤ，α）’になる。

また、受信装置においては、暗号ビット除去部１１から出力される信号（ＤＡ，ＩＤ）に対して判定部１５が次のような判定を行う。すなわち、判定部１５は、信号（ＤＡ，ＩＤ）中の識別情報ＩＤを読み、これが送信装置の識別情報と一致するかどうかを判定する。送信装置のＩＤは、事前の通信によって予め認識するか、あるいは、通信予定のある装置について、予め設定操作により登録しておく。

そして、判定部１５において、識別情報の一致が検出された場合には、正常な受信が行えたと判定し、受信信号に含まれる信号ＤＡを正規な情報として後段に

出力する。一方、判定部１５において、識別情報の一致が検出されない場合には、当該受信信号を無効にする。

以上のように、この変形例においては、乱数による信号の秘匿に加えて、識別情報の一致を判断しているので、妨害には極めて強いと言える。

なお、上記変形例において、パケット通信を行う場合には、パケットのヘッダー部分に装置を識別するための情報が含まれているから、これと暗号化された信号内の識別情報ＩＤとを比較してもよい。この場合には、秘匿化されないヘッダー内の識別情報は外部から容易に傍受することができるが、暗号化された信号内の識別情報ＩＤは知ることができないため、仮に、ヘッダー部分をまねた信号が伝送されても、当該受信信号は判定部１５において無効とされるため、妨害を未然に防止することができる。

Ｂ：第２実施例

次に、この発明の第２実施例について、図９、図１０を参照して説明する。図９は送信側の構成を、図１０は受信側の構成を各々示しており、第１実施例と共通の部分には同一の符号が付けてある。

図９に示す２０はメモリであり、乱数ビットの挿入位置を示す乱数位置情報ＲＰが複数記憶されている。この場合、乱数αは、図１１（ａ）、（ｂ）に示すように、乱数位置情報ＲＰによって示されるビット位置に挿入される。また、上述した変形例のように乱数が分割されて乱数α_1、α_2となる場合は、乱数位置情報もそれぞれに対応して設定され、図１１（ｃ）に示すように、乱数位置情報ＲＰ$_1$，ＲＰ$_2$となる。

図９に示す制御部２１は、送信データ発生部１が出力する信号ＤＡ（原文データ　に対して、メモリ２０から読み出した乱数位置情報ＲＰを付加して乱数ビット付加部２２に転送する。乱数ビット付加部２２は、信号ＤＡに対し、乱数位置情報ＲＰに示されるビット位置に乱数αを挿入する。そして、乱数αが付加された信号（ＤＡ，α）は、暗号化処理部２によって暗号化された後、信号（ＤＡ，α ’として出力される。

次に、図１０に示すメモリ３０には、前述したメモリ２０と同様に乱数位置情報ＲＰが複数記憶されている。この場合、メモリ２０の記憶内容と、メモリ３０

の記憶内容は全く同一になっている。制御部３１は、解読処理部１０によって解読された信号（ＤＡ，α）に、メモリ２０から読み出した乱数位置情報ＲＰ（またはＲＰ$_1$、ＲＰ$_2$）を付加して乱数ビット除去部３２に転送する。このとき、メモリ２０から読み出される乱数位置情報の順番は、送信側の制御部２１の読み出し順序と同じである。したがって、メモリ３０から読み出される乱数位置情報ＲＰは、受信した信号（ＤＡ，α）における乱数αの挿入位置を示す情報となる。そして、乱数ビット除去部３２は、乱数位置情報ＲＰの内容に基づいて、信号（ＤＡ，α）から乱数αを除去し、信号ＤＡ（原文）を出力する。

以上のように、この実施例においては、乱数の挿入される位置が適宜変化するので、信号の秘匿性は極めて高いものとなる。

なお、第２実施例においては、予めメモリに記憶させた乱数位置情報ＲＰに基づいて乱数の挿入位置を変えたが、これを時刻情報等に基づいて変えてもよい。要は、送信側と受信側とで認識する乱数位置の同期がとれていればよい。

Ｃ：第３実施例

次に、第３変形例について図１２、図１３を参照して説明する。なお、これらの図において前述した各実施例の各部に対応する部分には同一の符号を付けてその説明を省略する。

図１２に示す付与位置情報発生部４０は、乱数αの付与位置を示す乱数位置情報ＲＰを発生する。この場合の乱数位置情報ＲＰは、ランダムな値あるいは所定の規則にしたがって変化する値である。また、メモリ４１には、乱数位置情報ＲＰの初期値が記憶されている。制御部２１は、送信データ発生部１から信号ＤＡ（原文）が供給されると、メモリ４１から読み出した乱数位置情報ＲＰとともに、乱数ビット付加部４２および付与位置情報付加部４３に転送し、さらに、付与位置情報発生部４０が新たに作成した乱数位置情報ＲＰをメモリ４１に上書きする。

乱数ビット付加部４２は、前述した第２実施例の場合と同様にして、信号ＤＡの乱数位置情報ＲＰに対応した位置に乱数αを挿入し、信号（ＤＡ，α）を作成して出力する。また、付与位置情報付加部４３は、信号（ＤＡ，α）の所定位置に乱数位置情報ＲＰを付加し、信号（ＤＡ，α，ＲＰ）として出力する。この信号は、暗号化処理部２によって暗号化され、信号（ＤＡ，α，ＲＰ）´として、

図１３に示す受信側に転送される。

次に、図１３に示すメモリ５０には、乱数位置情報ＲＰの初期値が記憶されており、この値はメモリ４１と同じ値になっている。また、制御部３２は、解読処理部１０から信号（ＤＡ，α，ＲＰ）が供給されると、メモリ５０から読み出した乱数位置情報ＲＰとともに、乱数ビット除去部５１に転送する。乱数ビット除去部５１においては、前述した実施例と同様に乱数位置情報ＲＰを参照して乱数αを除去し、信号（ＤＡ，ＲＰ）を作成して付与位置情報除去部５２に転送する。付与位置情報除去部５２では、信号（ＤＡ，ＲＰ）から乱数位置情報ＲＰを弁別し、信号ＤＡを復元して出力するとともに、弁別した乱数位置情報ＲＰを制御部３２に転送する。また、制御部３２に転送された乱数位置情報ＲＰをメモリ５０に更新書き込みする。

以上のように、送信側では、次の信号に対応する乱数位置情報ＲＰを、前の信号に付加して送信し、また、受信側では一つ前の信号に付加されていた乱数位置情報ＲＰを用いて新たな受信信号から乱数αを除去しているので、送信側で用いた乱数位置情報ＲＰと受信側で用いた乱数位置情報ＲＰとは、常に一致することになる。

なお、上述の説明では、次の送信信号の乱数位置情報ＲＰをその前の送信信号に付加していたが、これに代えて、そのときの送信信号に用いた乱数位置情報ＲＰをそのまま当該信号に付加するように構成してもよい。ただし、信号の秘匿性は、上述した実施例の方が高い。

Ｄ：その他

（１）乱数について

上述した各実施例における乱数としては、周知の乱数発生回路で発生させたものを用いればよい。また、乱数テーブルをメモリに記憶し、これを適宜読み出して乱数発生してもよい。

また、正確には乱数とは言えない数値も使用することができる。例えば、タイマーが出力する時刻情報や、所定のクロックを順次カウントするカウンタの出力値を用いてもよい。

（２）暗号化について

暗号化についても、種々のアルゴリズムを用いることができる。また、暗号化は、暗号鍵の運用方法によって、秘密鍵方式と公開鍵方式の２つの大別されるが、本発明においては、そのどちらでも適用することができる。

この場合、秘密鍵方式は、予め送受信の双方に同一の鍵を備えなければならないが、高速処理の実現が可能であるため、実用的と言える。なお、秘密鍵方式における鍵については、送受信の双方で予め固定的に記憶しておくこともできるし、通信の開始時に鍵の配送を行うこともできる。

なお、秘密鍵方式の暗号化アルゴリズムとして良く知られているものに、ＦＥＡＬ（Fast Data Enciphement Algorithm）がある。このアルゴリズムについては、例えば、「暗号と情報セキュリティ」（辻井　重男、笠原　正雄　著：昭晃堂）の第４３～４９ページに詳しい説明がある。

（３）乱数ビット付加部の構成例

ここで、上述した各実施例における乱数ビット付加部６、２２，４２の構成例を図１４に示す。この図に示す回路においては、シフトレジスタ６０，６１に信号ＤＡおよび乱数αが転送される。シフトレジスタ６０，６１は、クロック発生回路６２からアンドゲート６３，６４を各々介して供給されるクロックＣＫに基づいて信号ＤＡおよび乱数αを１ビットづつシフトして出力する。また、カウンタ６６はクロックＣＫをサイクリックにカウントするもので、そのカウント周期は、信号ＤＡと乱数α（またはα_1、α_2）を合わせた長さに対応する。デコーダ６７は、カウンタ６６のカウント値をデコードするもので、乱数位置情報ＲＰ（またはＲＰ$_1$，ＲＰ$_2$）に対応したカウント値から乱数α（またはα_1、α_2）に対応したカウント値において“１”信号を出力し、その他のカウント値において“０”信号を出力する。このデコーダ６７の出力信号は、アンドゲート６４に供給されるとともに、インバータ６５を介してアンドゲート６３に供給される。

以上の構成によれば、乱数位置情報ＲＰで指定される乱数αのビット位置以外においては、デコーダ６７の出力信号が“０”になるため、アンドゲート６３が開、アンドゲート６４が閉になり、シフトレジスタ６０だけがシフト動作を行う。したがって、シフトレジスタ６０内の信号ＤＡがオアゲート６８を介して出力される。一方、乱数位置情報ＲＰ（またはＲＰ$_1$，ＲＰ$_2$）で指定される乱数α（ま

たはα_1、α_2）のビット位置においては、デコーダ６７の出力信号が“１”になるため、アンドゲート６３が閉、アンドゲート６４が開になり、シフトレジスタ６１だけがシフト動作を行う。したがって、乱数α（あるいは、α_1、α_2）がオアゲート６８から出力される。このようにして、信号ＤＡの所定位置に乱数αが付加された信号が作成される。

また、前述したビット付加部９は、乱数αに加えて識別情報ＩＤの付加も行うが、乱数αの付加部分については、上述の回路の構成で実現できる。

なお、上述した回路例は、あくまで一例であり、他の回路構成を用いてもよく、また、ソフトウエア処理によって実現してもよい。

（４）乱数ビット除去部の構成例

図１５は乱数ビット除去部１１，２２，３２，５１の構成例を示すブロック図である。

図に示す回路においては、シフトレジスタ７０に信号ＤＡと乱数αの合成されたデータが転送される。また、クロック発生回路７１から出力されるクロック信号ＣＫは、シフトレジスタ７０、カウンタ７２およびアンドゲート７５に転送される。カウンタ７２はクロックＣＫをサイクリックにカウントするもので、そのカウント周期は、信号ＤＡと乱数α（またはα_1、α_2）を合わせた長さに対応する。デコーダ７３は、カウンタ７２のカウント値をデコードするもので、乱数位置情報ＲＰ（またはＲＰ$_1$，ＲＰ$_2$）に対応したカウント値から乱数α（またはα_1、α_2）において“１”信号を出力し、その他のカウント値において“０”信号を出力する。このデコーダ７３の出力信号は、アンドゲート７４，７５に供給される。

上述した構成によれば、シフトレジスタ７０からは、クロック信号ＣＫに同期して信号（ＤＡ，α）が順次出力される。そして、乱数位置情報ＲＰで指定される乱数αのビット位置以外においては、デコーダ７３の出力信号が“１”になるため、アンドゲート７５が開になり、シフトレジスタ７６がシフト動作を行う。このとき、アンドゲート７４も開になっているため、シフトレジスタ７０から順次出力されるデータは、アンドゲート７４を介して順次シフトレジスタ７６に転送される。

一方、乱数位置情報ＲＰで指定される乱数αのビット位置においては、デコーダ７３の出力信号が“０”になるため、アンドゲート７４，７５が閉になり、シフトレジスタ７０だけがシフト動作を行う。したがって、シフトレジスタ７０から出力される乱数α（あるいは、α_1、α_2）は、アンドゲート７４を通過せずに破棄される。このとき、シフトレジスタ７６はシフト動作を行わないから、入力側空きビットは生じない。そして、乱数α以外のビット位置になると、再び、アンドゲート７４，７５が開になるとともに、シフトレジスタ７６がシフト動作を開始するので、信号ＤＡはシフトレジスタ７６に転送される。以上の動作により、シフトレジスタ７６内には信号ＤＡだけが抽出される。

なお、上述した回路例は、あくまで一例であり、他の構成構成でもよく、また、ソフトウエア処理によって実現してもよい。

Ｅ：効果

以上説明したように、上述した各実施例においては、信号に乱数を付して暗号化するので、１つの信号に対する暗号化の結果が複数パターン発生し、これにより、例えば、共通アクセスチャンネルを用いるために情報がオープンになる場合でも、伝送信号自体を良好に秘匿し、妨害を十分に押さえることができる。

産業上の利用可能性

この発明は、例えば、共通アクセスチャンネルに複数の移動局がアクセスする場合に用いて好適であり、その他秘匿が必要な通信用途に用いることができる。また、移動通信においてパケット通信を行う場合などにも適用することができる。

請 求 の 範 囲

1. 送信側は、

伝送すべき信号の所定位置に乱数のビットを付加するとともに、所定の鍵を用いて暗号化して送信し、

受信側は、

受信信号を前記所定の鍵を用いて暗号解読するとともに、解読後の信号の所定位置から前記乱数のビットを除去する

ことを特徴とする信号伝送方式。

2. 送信側は、

伝送すべき信号の所定位置に乱数のビットおよび自局を識別する識別情報のビットを付加するとともに所定の鍵を用いて暗号化して送信し、

受信側は、

受信信号を前記所定の鍵を用いて暗号解読するとともに、解読後の信号の所定位置から前記乱数のビットを除去し、かつ、前記識別情報が送信側の装置の識別情報と一致するか否かを判定し、一致する場合に正常受信したと判断することを特徴とする信号伝送方式。

3. 送信装置は、

所定ビットの乱数を発生する乱数発生手段と、

送信すべき信号を送出する送信信号発生手段と、

前記送信信号発生手段が出力する信号の所定位置に前記乱数発生手段が発生した乱数のビットを付加して出力する乱数付加手段と、

前記乱数付加手段の出力信号を所定の鍵を用いて暗号化する暗号化手段と、

を具備し、

受信装置は、

前記所定の鍵を用いて受信信号の暗号を解いて出力する暗号解読手段と、

前記暗号解読手段の出力信号の所定位置から乱数のビットを除去して出力する乱数ビット除去手段と

を具備することを特徴とする通信システム。

4. 送信装置は、

所定ビットの乱数を発生する乱数発生手段と、

伝送すべき信号を送出する送信信号発生手段と、

前記送信信号発生手段が出力する信号の所定位置に前記乱数発生手段が発生した乱数のビットおよび自装置を識別するための識別情報のビットを付加して出力するビット付加手段と、

前記ビット付加手段の出力信号を所定の鍵を用いて暗号化する暗号化手段と、

を具備し、

受信装置は、

前記所定の鍵を用いて受信信号の暗号を解いて出力する暗号解読手段と、

前記暗号解読手段の出力信号の所定位置から乱数のビットを除去する乱数ビット除去手段と、

前記暗号解読手段の出力信号に含まれる識別情報が前記送信装置の識別情報と一致するか否かを判定し、一致していた場合に当該受信信号を有効と判定する判定手段と

を具備することを特徴とする通信システム。

5. 送信側は、乱数のビットを付加する位置を示す乱数位置情報を発生し、この乱数位置情報に応じたビット位置に乱数を付加し、

受信側は、送信側と同じ値の乱数位置情報を送信側と同じ順序で発生し、乱数ビットを除去する際には、発生した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする請求項1または2記載の信号伝送方式。

6. 前記送信装置は、

乱数のビットを付加する位置を示す乱数位置情報を発生する第1の乱数位置情報発生手段を有し、前記乱数付加手段は前記第1の乱数位置情報発生手段が発生した乱数位置情報に応じた位置に前記乱数を付加し、

前記受信装置は、

前記第1の乱数位置情報発生手段が発生する位置情報と同じ値の位置情報を同じ順序で発生する第2の乱数位置情報発生手段を有し、前記乱数ビット除去手段は前記第2の乱数位置情報発生手段が発生した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする請求項3または4記載の通信システム。

7. 前記送信側は、乱数のビットを付加する位置を示す乱数位置情報を発生し、この乱数位置情報に応じたビット位置に乱数を付加するとともに、前記送信信号に前記乱数位置情報を付加し、

前記受信側は、受信信号から乱数位置情報を抽出し、乱数ビットを除去する際には、抽出した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする請求項1または2記載の信号伝送方式。

8. 前記送信装置は、

乱数のビットを付加する位置を示す乱数位置情報を発生する乱数位置情報発生手段と、前記乱数位置情報を前記送信信号に付加する乱数位置信号付加手段とを有し、前記乱数付加手段は前記乱数位置情報発生手段が発生した乱数位置情報に応じた位置に前記乱数を付加し、

前記受信装置は、

前記受信信号から乱数位置情報を抽出する乱数位置情報抽出手段を有し、前記乱数ビット除去手段は前記乱数位置情報抽出手段が抽出した乱数位置情報に対応するビット位置から乱数を除去することを特徴とする請求項3または4記載の通信システム。

9. 前記送信側は、次に送信すべき送信信号の乱数位置情報を、その直前に送信する送信信号に付加し、

前記受信側は、直前の受信信号から抽出した乱数位置情報に基づいて次の受信信号から乱数を除去することを特徴とする請求項7記載の信号伝送方式。

10. 前記送信装置の乱数付加手段は、次に送信すべき送信信号の乱数位置情報を、その直前に送信する送信信号に付加し、

前記受信装置の乱数ビット除去手段は、前記乱数位置情報抽出手段が直前の受信信号から抽出した乱数位置情報に基づいて次の受信信号から乱数を除去することを特徴とする請求項8記載の通信システム。

図 1

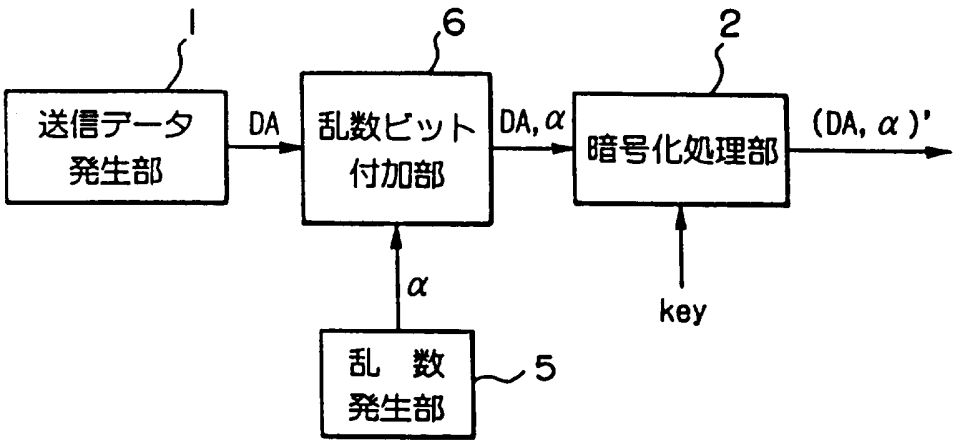

1
6
2
送信データ発生部
DA
乱数ビット付加部
DA, α
暗号化処理部
(DA, α)'
α
key
乱 数 発生部
5

図 2

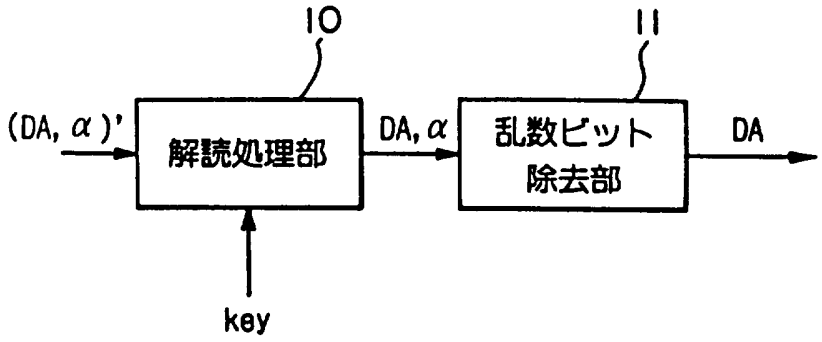

10
11
(DA, α)'
解読処理部
DA, α
乱数ビット除去部
DA
key

図 3

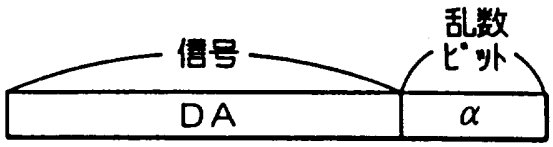

信号
乱数ビット
DA
α

図 4

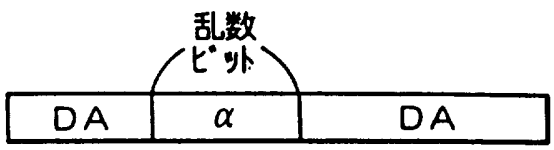

乱数ビット
DA
α
DA

図 5


DA
α_1
DA
α_2

図 6

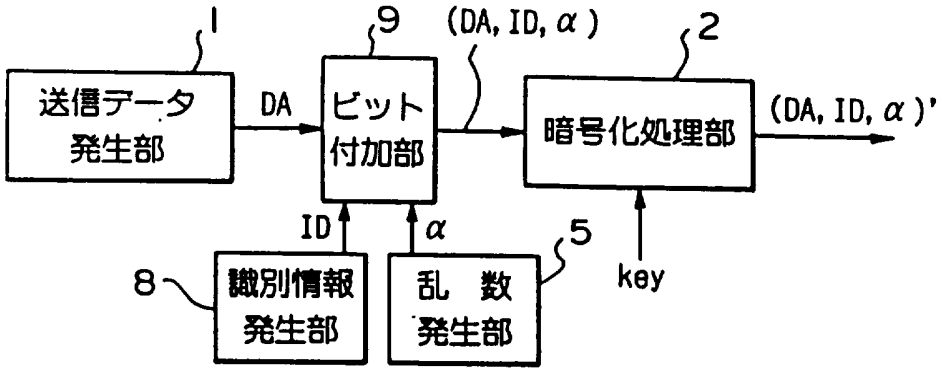

1
9
(DA, ID, α)
2
送信データ発生部
DA
ビット付加部
暗号化処理部
(DA, ID, α)'
ID
α
5
key
8
識別情報発生部
乱 数発生部

図 7

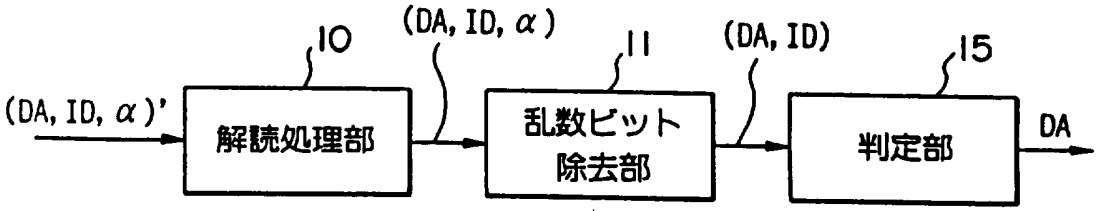

10
(DA, ID, α)
11
(DA, ID)
15
(DA, ID, α)'
解読処理部
乱数ビット除去部
判定部
DA

図 8


DA
ID
α

図 9

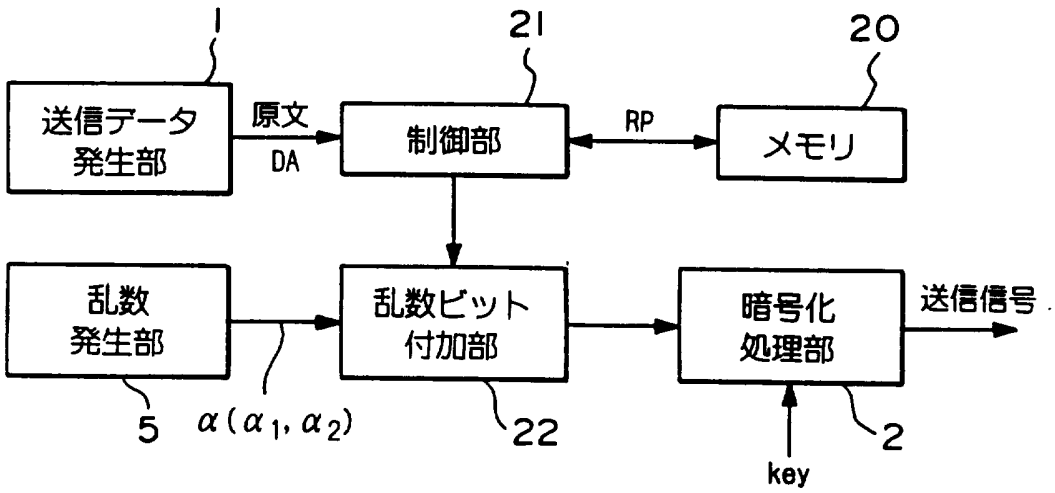

1
21
20
送信データ
発生部
原文
DA
制御部
RP
メモリ
乱数
発生部
乱数ビット
付加部
暗号化
処理部
送信信号
5
α(α1, α2)
22
2
key

図10

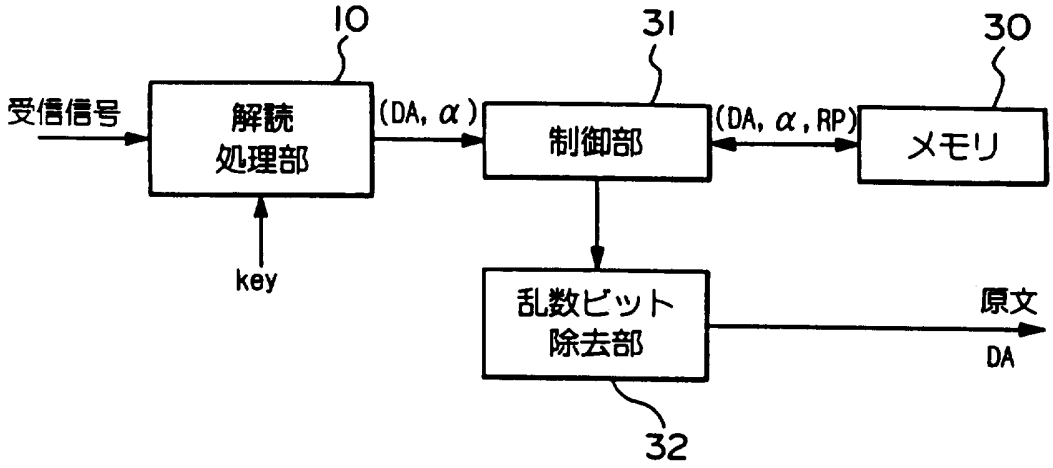

10
31
30
受信信号
解読
処理部
(DA, α)
制御部
(DA, α, RP)
メモリ
key
乱数ビット
除去部
原文
DA
32

図１１

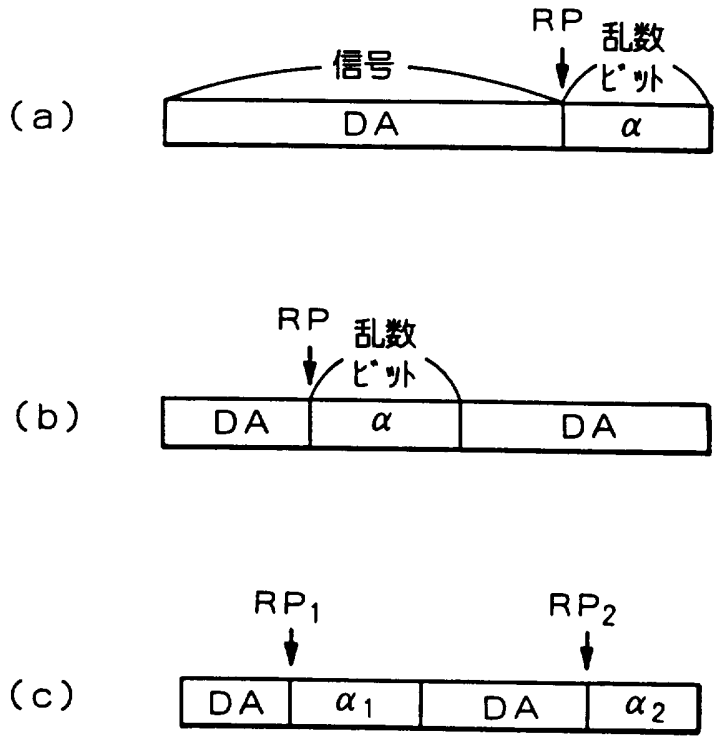


図12

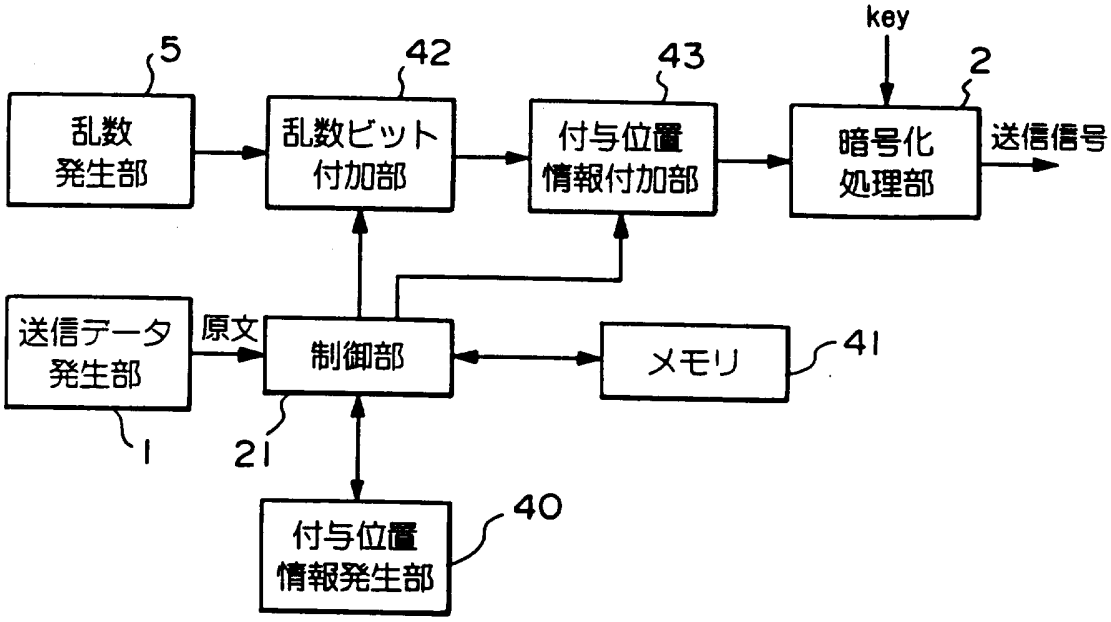

5
42
43
key
2
乱数
発生部
乱数ビット
付加部
付与位置
情報付加部
暗号化
処理部
送信信号
送信データ
発生部
原文
制御部
メモリ
41
1
21
付与位置
情報発生部
40

図13

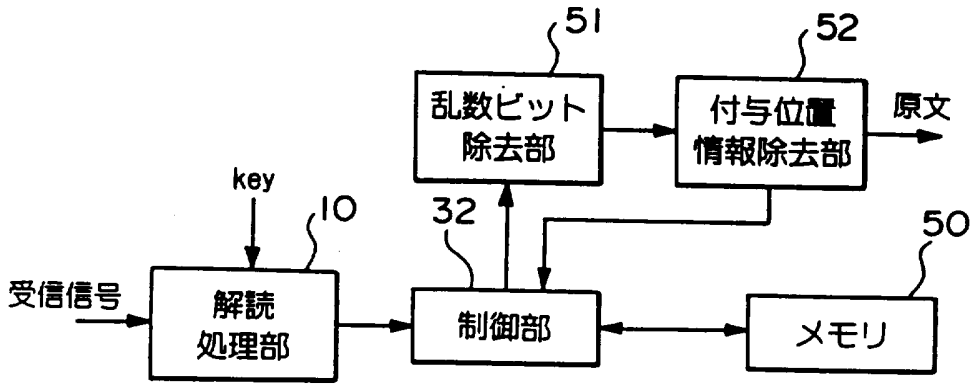

51
52
乱数ビット
除去部
付与位置
情報除去部
原文
key
10
32
50
受信信号
解読
処理部
制御部
メモリ

図14

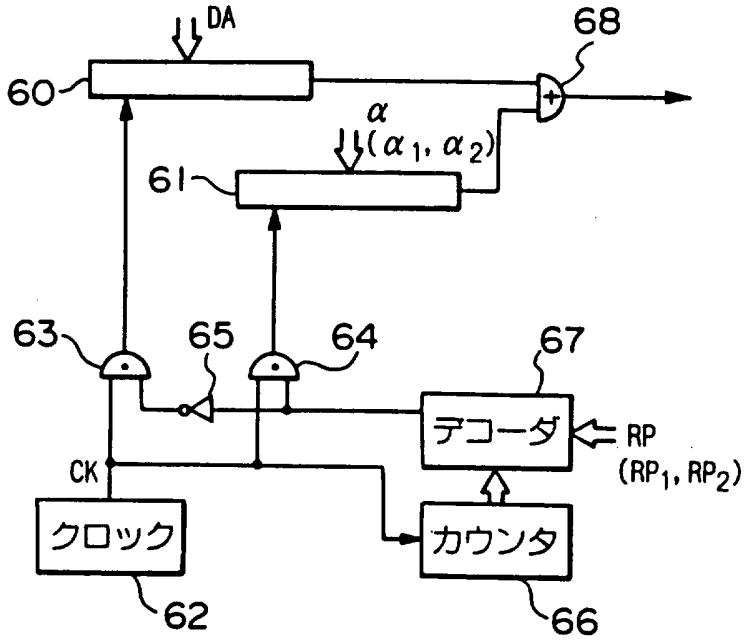

DA
68
60
α
(α1, α2)
61
63
65
64
67
デコーダ
RP
(RP1, RP2)
CK
クロック
カウンタ
62
66

図15

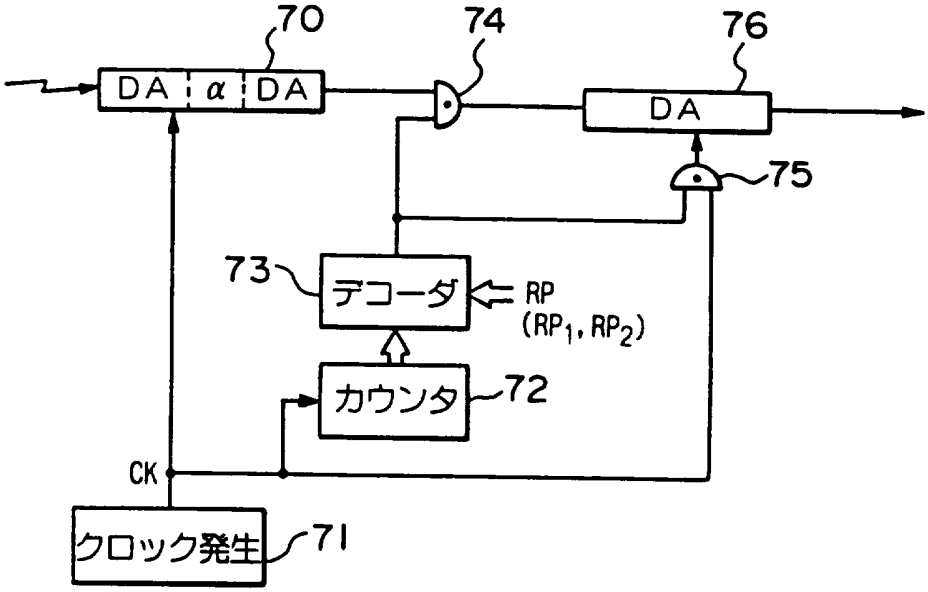
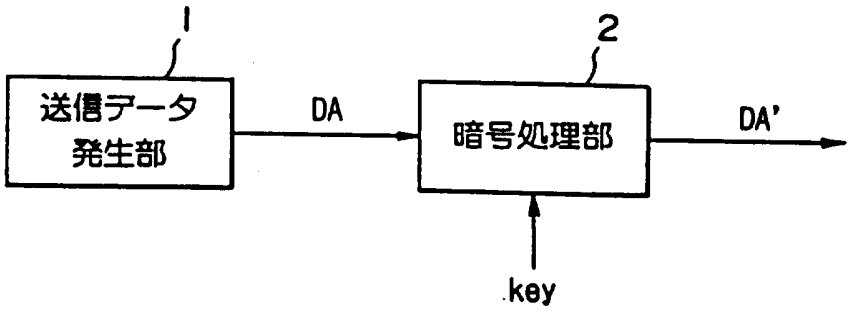

70
74
76
DA
α
DA
DA
75
73
デコーダ
RP
(RP1, RP2)
カウンタ
72
CK
クロック発生
71

図16



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/01410

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl^6 H04L9/28

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)

Int. Cl^6 H04L9/00, H04K1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926 - 1995
Kokai Jitsuyo Shinan Koho 1971 - 1995

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 4-101529, A (Nittsuko K.K.), April 3, 1992 (03. 04. 92), Line 5, lower left column to line 10, lower right column, page 2, line 16, upper left column to line 1, upper right column, page 3 (Family: none)	1 - 10
Y	JP, 1-194627, A (NEC Corp.), August 4, 1989 (04. 08. 89), Line 8, lower right column, page 1 to line 13, upper left column, page 2 (Family: none)	1 - 10
Y	JP, 63-248240, A (Canon Inc.), October 14, 1988 (14. 10. 88), Line 2, upper left column to line 8, upper right column, page 2, lines 12 to 16, lower right column, page 2 (Family: none)	1 - 10
Y	JP, 1-284037, A (NEC Corp.), November 15, 1989 (15. 11. 89), Line 2, upper left column, page 2 to line 8,	9 - 10

[X] 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 document 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
September 21, 1995 (21. 09. 95)	October 9, 1995 (09. 10. 95)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP95/01410

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	upper left column, page 3 (Family: none)	
Y	JP, 1-212039, A (Toshiba Corp.), February 14, 1989 (14. 02. 89), Claim (Family: none)	2, 4-10

国際調査報告

国際出願番号 PCT/JP 95/01410

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶ H04L9/28

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. Cl⁶ H04L9/00, H04K1/00

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 1926－1995年

日本国公開実用新案公報 1971－1995年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 4－101529, A（日通工株式会社）, 3. 4月. 1992（03. 04. 92）, 第2頁左下欄第5行－同右下欄第10行, 第3頁左上欄第16行－同右上欄1行（ファミリーなし）	1－10
Y	JP, 1－194627, A（日本電気株式会社）, 4. 8月. 1989（04. 08. 89）, 第1頁右下欄第8行－第2頁左上欄第13行（ファミリーなし）	1－10

☑ 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」先行文献ではあるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
21. 09. 95	09.10.95

名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA/JP） 郵便番号100 東京都千代田区霞が関三丁目4番3号	吉見信明 ㊞	5K 2116
	電話番号 03－3581－1101 内線	3557

様式PCT/ISA/210（第2ページ）（1992年7月）

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	関連する請求の範囲の番号
Y	JP，63－248240，A（キヤノン株式会社），14．10月 1988（14．10．88），第2頁左上欄第2行－同右上欄第8行及び同右下欄第12行－第16行（ファミリーなし）	1－10
Y	JP，1－284037，A（日本電気株式会社），15．11月 1989（15．11．89），第2頁左上欄第2行－第3頁左上欄第8行（ファミリーなし）	9－10
Y	JP，1－212039，A（株式会社　東芝），19．2月 1989（19．02．89），特許請求の範囲（ファミリーなし）	2，4－10