(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-526453
(P2005-526453A)
(43)公表日　平成17年9月2日(2005.9.2)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04N 7/167	H04N	7/167	Z	5C025
H04N 5/44	H04N	5/44	Z	5C064
H04N 7/173	H04N	7/173	630	

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

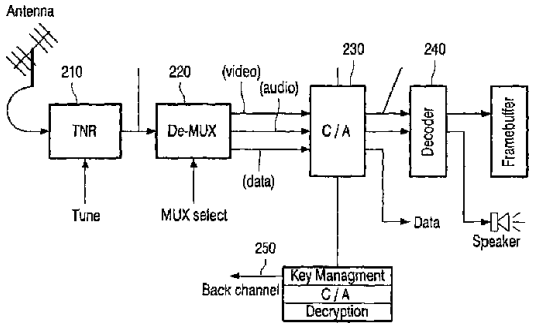
(21)出願番号　特願2004-506281 (P2004-506281)
(86)(22)出願日　平成15年4月23日 (2003.4.23)
(85)翻訳文提出日　平成16年11月18日 (2004.11.18)
(86)国際出願番号　PCT/IB2003/001713
(87)国際公開番号　WO2003/098919
(87)国際公開日　平成15年11月27日 (2003.11.27)
(31)優先権主張番号　02076984.0
(32)優先日　平成14年5月21日 (2002.5.21)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100092048
弁理士　沢田　雅男

最終頁に続く

(54)【発明の名称】条件付きアクセス・システム

(57)【要約】
【課題】スクランブル化された複数のストリームを扱うことにより適したブロードキャスト受信器を提供すること。
【解決手段】　ブロードキャスト受信器には、複数のブロードキャスト・デジタル・トランスポート・ストリームの少なくとも1つに選択的にチューニングし、かつこのチューニングされたトランスポート・ストリームを複数の並列な非多重化されたデータ・ストリームに非多重化して、非多重化されたデータ・ストリームの少なくとも1つを選択的に提供するチューナ／デマルチプレクサ410、420が含まれている。非多重化されたデータ・ストリームは、時間によって変わるコンテンツ鍵の制御下でスクランブル化されていてもよい。チューナ／デマルチプレクサは、このチューニングされたトランスポート・ストリームから、少なくとも2つのスクランブル化された非多重化されたデータ・ストリームに対して各々の制御ワード・ストリーム510、520、530を抽出する。各制御ワードは、暗号化されたコンテンツ鍵を表している。制御器は、この制御ワード・ストリームからデクリプタ



【特許請求の範囲】
【請求項１】
少なくとも1つのチューナ／デマルチプレクサ、少なくとも1つのデスクランブラ、および少なくとも1つのデクリプタを含む、ブロードキャスト・データ・ストリームに対する条件付きアクセスを行うためのブロードキャスト受信器であって、
前記チューナ／デマルチプレクサが、
複数のブロードキャスト・デジタル・トランスポート・ストリームの内の少なくとも1つを選択的にチューニングし、
非多重化されたデータ・ストリームの内の少なくとも1つを選択的に提供するために、
非多重化された1データ・ストリームが、時間によって変わるコンテンツ鍵の制御下でスクランブル化されていてもよい、非多重化された複数の並列なデータ・ストリームに、前記チューニングされたトランスポート・ストリームを非多重化して、
少なくとも2つのスクランブル化されている非多重化されたデータ・ストリームに対して、各制御ワードが暗号化されたコンテンツ鍵を表す、個々の制御ワード・ストリームを、前記チューニングされたトランスポート・ストリームから抽出し、かつ、
前記制御ワード・ストリームを提供するように動作し、
前記デクリプタが、制御ワードを対応するコンテンツ鍵に復号化するように動作し、
前記ブロードキャスト受信器が、
前記チューナ／デマルチプレクサから前記複数の制御ワード・ストリームを受信し、
前記制御ワード・ストリームの制御ワードを前記デクリプタに供給し、
前記供給された制御ワードの各々に対して、対応するコンテンツ鍵を前記デクリプタから取り出し、
各制御ワード・ストリームに対して、対応するコンテンツ鍵ストリームを形成し、
各コンテンツ鍵ストリームに対して、少なくとも1つの最新のコンテンツ鍵をメモリ内に格納し、かつ、
選択された非多重化されたデータ・ストリームに対して、前記選択された非多重化されたデータ・ストリームに関連付けられた前記コンテンツ鍵を前記メモリからデスクランブラに提供して、前記デスクランブラが前記データ・ストリームをデスクランブル化することを可能にする、
ように動作する制御器を更に含んでおり、かつ、
前記デスクランブラが、前記対応するコンテンツ鍵のストリームのコンテンツ鍵の制御下にある選択された非多重化されたデータ・ストリームをデスクランブル化するように動作する、
ブロードキャスト受信器。
【請求項２】
前記チューナ／デマルチプレクサが、複数の選択された非多重化されたデータ・ストリームを提供するように動作し、かつ、
前記デスクランブラが、前記選択されたストリームの各々に対する、前記メモリから供給されるコンテンツ鍵の制御の下、前記複数の非多重化されたデータ・ストリームをデスクランブル化するように動作する、
請求項１に記載の受信器。
【請求項３】
前記デスクランブラが、前記複数の選択された非多重化されたデータ・ストリームのデスクランブリングを時間多重化で行うように動作し、
前記チューナ／デスクランブラにより提供された前記複数の非多重化されたデータ・ストリームが、一時的にバッファリングされて、時間多重化されたストリームとして前記デスクランブラに供給され、
前記制御器が、前記選択された非多重化されたデータ・ストリームの内の異なる1ストリームからデスクランブル・データへのスイッチングを前記デスクランブラと同期して行

わせ、前記選択された非多重化されたデータ・ストリームの内の前記異なるストリームに対する、前記メモリからのコンテンツ鍵を、前記デスクランブラへロードするように動作する、
請求項2に記載の受信器。
【請求項４】
前記制御器が、デスクランブル化された形態で供給される次のデータ・ストリームを予測し、
前記予測されたデータ・ストリームに対する制御ワード・ストリームを前記チューナ／デマルチプレクサに提供させ、かつ、
前記データ・ストリームの実際の選択に応答して、前記新たに選択されたデータ・ストリームを前記デスクランブラに供給することを、前記データ・ストリームに対する、前記メモリ内に格納されているコンテンツ鍵の供給に同期して行わせる、
ように動作する、請求項1に記載の受信器。
【請求項５】
前記制御器が、
前記複数の制御ワード・ストリームの制御ワードを、前記デクリプタへシーケンシャルに供給するためにシーケンス状に構成し、前記デクリプタが前に供給された制御ワードの復号化を完了させて初めて、前記シーケンスの次の制御ワードが供給される、
ように動作する、請求項１に記載の受信器。
【請求項６】
前記制御器が、新たに提供された制御ワード・ストリームの制御ワードのシーケンスを優先させるように動作する、請求項５に記載の受信器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、条件付きアクセス・システム、具体的にはデジタル・オーディオ／ビデオ・データなどのブロードキャスト・データに対する条件付きアクセスを行うためのブロードキャスト受信器に関する。
【背景技術】
【０００２】
デジタル・オーディオ／ビデオ伝送システムは、オーディオ／ビデオ・チャネルのブロードキャストにますます利用されて来ている。デジタル・ビデオ・ブロードキャスティング (DVB: Digital Video Broadcasting) システムを一例にとると、ネットワーク・プロバイダは、多数のサービスを各々が含んでいる多数のトランスポート・ストリームをブロードキャストする。トランスポート・ストリームは、通常、別個の周波数帯域で伝送され（周波数多重化）、サービスは、時間多重化を用いてストリームにコード化される。サービスはたいていチャネルと称される。受信器には、特定のトランスポート・ストリームにチューニングするためのチューナ、およびこのストリームから特定のサービス／チャネルを抽出するためのデマルチプレクサ (demultiplexer) が含まれている。DVBの場合、A/VストリームはMPEG-2でコード化される。トランスポート・ストリームは、MPEG-2でコード化されたデータ・ストリームを多重化 (multiplex) したものである。受信器内では、デマルチプレクサにより抽出されたデータ・ストリームはMPEG-2でデコードされて、レンダリングに適した形態（例えば、表示装置上に表示させるためのアナログ形態）となる。ある種の受信器の場合、ユーザが1つのチャネルをビューしながら異なるチャネルを同時に記録することができるように、チューナ／デマルチプレクサ／デコーダの組が2つ用いられる。
【０００３】
従来のブロードキャスト・システムの場合、データは伝送器により複数の受信器へブロードキャストされる。データへのアクセスは条件付きにして、例えば、特定の受信器に対して視聴料が支払済みか否かということに依存させることができる。データ・サービスに

対するこのような条件付きアクセスは、権限鍵の制御の下でデータをスクランブル化（暗号化）すること、およびこのスクランブル化されたデータを受信器に伝送することにより実現される。スクランブル化は通常、伝送器内で行われる。データのデスクランブル化（複合化）に必要な復号鍵自体は暗号化（encrypt）され、かつ受信器に伝送される。暗号鍵と復号鍵が同一の対称暗号化技法がたいてい用いられる。データに対する資格を有する受信器しか、デクリプタ（decryptor）を用いて復号鍵を復号化（decrypt）することができない。次に受信器は、データを復号化するためのデスクランブラを用いて、データをデスクランブル化することができる。デスクランブラは、暗号化に使用されたものと同一の権限鍵の制御の下、データブロックを復号化する。権限鍵の暗号化／復号化は通常、安全な環境内で行われる。このためにこれらの機能はたいてい、受信器内のスマートカード上、または受信器に接続されたスマートカード上で実行される。権限鍵を用いて、データ・ストリームの暗号化／復号化を直接制御してもよい。しかしながら、デクリプタからデスクランブラに送信された権限鍵を悪意のユーザが取り出して、かつこの鍵を他の受信器のデスクランブラに供給してしまうことがないように、セキュリティ・レイヤを１つ以上追加することが好ましい。このようなシステムでは、データをスクランブル化／デスクランブル化するために使用される鍵は、頻繁に（例えば、10秒毎に）変更される。この鍵はたいていコンテンツ鍵と称される。このコンテンツ鍵自体も、暗号化を制御する権限鍵を用いて暗号化された（制御ワードと称される）形態で、全ての受信器に伝送される（通常はブロードキャストされる）。このシナリオの場合、権限鍵は、制御ワードの復号化を直接制御し、かつデータのデスクランブル化を間接的に制御する。受信器の安全なモジュール内では、制御ワードの復号化も行われる。したがって、制御ワードの復号化には相当量の時間（例えば、300～600 m秒）がかかってしまう。また従来のブロードキャスト受信器は、スクランブル化されたストリームを1つ扱うようにしか設計されていない。

【発明の開示】

【課題を解決するための手段】

【０００４】

本発明の目的は、スクランブル化された複数のストリームを扱うことにより適したブロードキャスト受信器を提供することである。

【０００５】

本発明のこの目的を達成するために、

ブロードキャスト・データ・ストリームに対する条件付きアクセスを行うためのブロードキャスト受信器は、少なくとも1つのチューナ／デマルチプレクサ、少なくとも1つのデスクランブラ、および少なくとも1つのデクリプタを含み、

前記チューナ／デマルチプレクサは、

複数のブロードキャスト・デジタル・トランスポート・ストリームの内の少なくとも1つを選択的にチューニングし、

非多重化（demultiplex）されたデータ・ストリームの内の少なくとも1つを選択的に提供するために、非多重化された1データ・ストリームは、時間によって変わるコンテンツ鍵の制御下でスクランブル化されていてもよい、非多重化された複数の並列なデータ・ストリームに、前記チューニングされたトランスポート・ストリームを非多重化して、

少なくとも2つのスクランブル化されている非多重化されたデータ・ストリームに対して、各制御ワードが暗号化されたコンテンツ鍵を表す、個々の制御ワード・ストリームを、前記チューニングされたトランスポート・ストリームから抽出し、かつ、

前記制御ワード・ストリームを提供するように動作し、

前記デクリプタは、制御ワードを対応するコンテンツ鍵に復号化するように動作し、

前記ブロードキャスト受信器は、

前記チューナ／デマルチプレクサから前記複数の制御ワード・ストリームを受信し、

前記制御ワード・ストリームの制御ワードを前記デクリプタに供給し、

前記供給された制御ワードの各々に対して、対応するコンテンツ鍵を前記デクリプタから取り出し、

各制御ワード・ストリームに対して、対応するコンテンツ鍵ストリームを形成し、

各コンテンツ鍵ストリームに対して、少なくとも1つの最新のコンテンツ鍵をメモリ内に格納し、かつ、

選択された非多重化されたデータ・ストリームに対して、前記選択された非多重化されたデータ・ストリームに関連付けられた前記コンテンツ鍵を前記メモリからデスクランブラに提供して、前記デスクランブラが前記データ・ストリームをデスクランブル化することを可能にする、

ように動作する制御器を更に含んでおり、かつ、

前記デスクランブラは、前記対応するコンテンツ鍵のストリームのコンテンツ鍵の制御下にある選択された非多重化されたデータ・ストリームをデスクランブル化するように動作する。

【０００６】

本発明によると、デマルチプレクサは、複数のデータ・ストリームに対して、対応する制御ワード・ストリームを供給する。デクリプタは、様々な異なるストリームに対する制御ワードをコンテンツ鍵に復号化するために使用される。ストリーム毎に、少なくとも1つの最近のコンテンツ鍵がメモリ内に格納される。このように受信器は、複数のデータ・ストリームに対処できるコンテンツ鍵を持ち、このようなストリームの実際のデスクランブル処理をより速やかに開始させることができるので、デスクランブル化を高速に行うことが可能となる。

【０００７】

従属請求項2に記載されているように、複数のデータ・ストリームをレンダリングすべき出力として選択して（この出力は、例えば、ビューされたりまたは後でビューするために格納される）、選択された全てのストリームに対して、既に準備されているコンテンツ鍵がデスクランブラに供給される。こうして、複数ストリームを並列にデスクランブル化することが可能となる。

【０００８】

従属請求項3に記載の好ましい一実施例の場合、デスクランブラは、この並列デスクランブル化を時間多重化による手法で行う。デスクランブラが、新たなデータ・ストリームの「時間片（time-slice)」を処理し始める度に、このストリームに対するコンテンツ鍵がロードされる。

【０００９】

従属請求項4に記載されているように、視聴者が次に選択したいと思う可能性のあるチャネル（例えば、現在のチャネルより１つだけ高いチャネル）が、予測される。予測されたチャネルのために、デマルチプレクサが早くも制御ワードのストリームを供給し、かつ復号化された最新の制御ワード（コンテンツ鍵）が格納される。その後、予測されたチャネルをユーザが実際に選択した時点で、コンテンツ鍵がデスクランブラに「直ちに」供給されるので、ユーザは非常に速くチャネルにアクセスすることができる。

【００１０】

従属請求項5に記載されているように、受信器の制御器は、様々な制御ワード・ストリームに合わせてデクリプタを用いるように管理する。この制御器は、ストリームの内の1つに対する制御ワードの復号化が、別のストリームに対する制御ワードの復号化要求により中断されることがないようにする。非多重化された全てのデータ・ストリームと、これらの各々の制御ワード・ストリームとは原則的には非同期だが、デクリプタへのアクセスはこのようにして同期化される。

【００１１】

従属請求項6に記載されているように、制御器により新たに受信された制御ワード・ストリームが優先される。例えば、新たなチャネルがユーザにより選択された場合、制御器は、ユーザがもっとも選択しそうな次の候補として別のチャネルを予測してもよい。次に制御器は、デマルチプレクサに命令して、この予測されたチャネルに対する制御ワードを供給させることができる。優先される新たな制御ワード・ストリームの第一制御ワードを

復号化することにより、予測されたチャネルをデスクランブル化するためのコンテンツ鍵が、可能な限り早く利用可能となる。こうして、ユーザはより速くザッピングすることができる。

【００１２】

本発明のこれらの態様と他の態様は、以下に記載する実施例から、かつこれらの実施例を参照することにより明らかとなるであろう。

【発明を実施するための最良の形態】

【００１３】

図1は、本発明による受信器を使用することができる、デジタル・テレビ・システムの概要を示している。一例として、A/V信号を圧縮するMPEG-2圧縮を用いてオーディオ／ビデオ（A/V）信号がデジタル的に配信されるシステムを説明する。このシステムには、通常はブロードキャスト・センタに位置付けられるMPEG-2コンプレッサ10が、含まれている。このコンプレッサは、デジタル信号ストリーム（通常はデジタル化されたアナログまたはデジタルのビデオ信号によるストリーム）を受信する。元の信号は、サービス・プロバイダにより供給される。コンプレッサは、スクランブラとマルチプレクサ（multiplexer）20に接続されている。以下に詳述するように、スクランブラは、データ・ストリームのデジタル信号のスクランブル化を、これらの信号をコンテンツ鍵の制御下で暗号化することにより行う。マルチプレクサ20は、1つ以上のスクランブル化されたデータ・ストリームまたはスクランブル化されていないデータ・ストリームに加えて、更なるデジタル信号を受信してもよい。マルチプレクサ20は、全ての信号とストリームをトランスポート・ストリームにアセンブルし、かつ圧縮と多重化が行われた信号をブロードキャスト・センタの伝送器30に供給する。スクランブル化機能と多重化機能は別々のユニット内で行ってもよく、かつ必要に応じて異なる場所で行ってもよい。多重化されたトランスポート・ストリームは、通信リンクなどの任意の適切な形態の結合を用いて、スクランブラ／マルチプレクサ20から伝送器30に供給してもよい。伝送器30は、アップリンクを介して電磁信号を衛星トランスポンダ40へ伝送する。衛星トランスポンダ40では、電磁信号が電子的に処理され、かつダウンリンクを介して（従来はエンド・ユーザのパラボラアンテナの形態をした）地球ベースの衛星受信器50へブロードキャストされる。図中、衛星受信器50は統合型受信器60に接続されている。以下、図2を参照しながら受信器60の動作を詳述する。この受信器は、所望の信号を選択し、かつテレビジョン70などのレンダリング・デバイスにこの信号を適切な形態で提示する。勿論、この信号は、テープ記録装置、光ディスク記録装置またはハードディスク記録装置、もしくは他の適切な記録装置を用いて記録してもよい。この信号は、CATVケーブルまたはIEEE 1394などの周知の配信システムを用いて、アナログまたはデジタルの形態でレンダリング／記録用のデバイスに供給してもよい。デジタル配信の場合、非多重化された信号は、トランスポート・ストリームを部分的に用いるMPEG-2コーディングで供給されるので、トランスポート・ストリームを部分的にデコードするだけでよい。

【００１４】

配信の大部分は衛星を介して行う必要がないことが理解されるであろう。この代わりに、地上ブロードキャスト、ケーブル伝送、衛星／ケーブルの結合体などの他の配信システム（つまり、多重化されたものが1つ以上伝送される物理的媒体）を利用してもよい。配信システムを介してプログラムを配信する当事者は、ネットワーク・プロバイダと称されることがある。更に、受信器／デコーダ60をレンダリング・デバイスまたは記録用デバイスに統合化してもよいことが理解されるであろう。

【００１５】

典型的なシステムは、マルチチャネル・システムとして動作する。このことは、マルチプレクサ20が、多数の（並列な）ソースから受信されたA/V情報を取り扱うことができ、かつ伝送器30と相互作用して、対応する数のチャネル沿いにこの情報をブロードキャストさせたり、または別々のトランスポート・ストリームに多重化させることを示唆している。伝送されるデジタル・オーディオ／ビデオ情報がインターレースされるこれらのサービ

ス／チャネルの幾つかまたは全てには、A/V信号に加えて、メッセージもしくはアプリケーションまたは他のいかなる種類のデジタル・データを導入してよい。このように、トランスポート・ストリームには、1つ以上のサービス構成要素を各々有する1つ以上のサービスが含まれている。サービス構成要素は、単一媒体の要素である。サービス構成要素の例として、ビデオ基本ストリーム、オーディオ基本ストリーム、Java（登録商標）アプリケーション（Xlet)、または他のデータ・タイプが挙げられる。トランスポート・ストリームは、1つ以上の基本ストリームおよび／または基本データを時間多重化することより形成される。

【００１６】

図2は、典型的なブロードキャスト受信器の更なる詳細を示している。ブロードキャストされた受信器にはチューナ210が含まれている。チューニング可能な別々の無線周波数(RF) バンドをチューナ210が抽出すると、通常はMPEG2トランスポート・ストリームが得られる。デマルチプレクサ220 (De-MUX) により、一定のキャリア信号から可変データ信号が分離される。この結果多くの場合、オーディオ出力、ビデオ出力、およびデータ出力が得られる。ビデオ・ストリームとオーディオ・ストリームは、アクセス許可を決定しかつデータを復号化することができる条件付きアクセス・サブシステム230を通してフィードしてもよい。復号化されたオーディオ／ビデオ・ストリームは、デコーダ240にフィードされる。デコーダ240は、これらのストリームを、ビデオとオーディオのレンダリング、または格納デバイスに適した信号に変換する。この変換には、MPEG2デコーディングが関与してもよい。バック・チャネル250は存在しても存在しなくてもよい。バック・チャネル250が存在する場合、データは、サービス・プロバイダのサーバに伝送されて、相互作用テレビ、電子商取引などの相互作用アプリケーションを促進する。

【００１７】

上述したようなブロードキャスト・システムでは、受信器の限られた数のユーザ（例えば、支払い済みのユーザまたは特定グループに属するユーザ）しかデータ・サービスの幾つかまたは全てにアクセスできないことが望ましい。データ・サービスに対するこのような条件付きアクセスは、データを暗号化すること、およびこの暗号化されたデータを受信器へ伝送することを、図1の伝送器30に行わせることにより実現される。データの暗号化は、図1に示すスクランブリング・システム20を用いて伝送システム内で行い、かつ復号化は図2の条件付きアクセス・サブシステム230を用いて行ってもよい。図3には、典型的なスクランブリング・システムの更なる詳細が示されている。ここでデータは、コンテンツ・エンクリプタ310を用いて伝送サブシステム300内で暗号化される。このようなエンクリプタ (encryptor) 310は、たいていスクランブラと称される。実際のスクランブル化が先に行われている場合、暗号化されたデータを必要に応じて伝送サブシステムに供給してもよい。データは、コンテンツ鍵により直接制御されて暗号化される。典型的なシステムでは、コンテンツ鍵は例えば、10秒毎に変わる。コンテンツ鍵は、権限鍵の制御下で暗号化された暗号化された形態で、伝送器により受信器に供給される。このために、伝送サブシステムは、コンテンツ鍵を暗号化するエンクリプタ320を含んでいる。暗号化されたコンテンツ鍵は、制御ワード (CW: control word) と称される。制御ワードは、通常、いわゆる資格制御メッセージ (ECM: Entitlement Control Message) 内で伝送される。このようなECMは、IPパケットまたはMPEGトランスポート・ストリーム内に埋め込んでもよい。同一のECMが全ての受信器に送信（ブロードキャスト）される。受信器の条件付きアクセス (CA) サブシステム350には、暗号化されている制御ワードを復号化するデクリプタ370が含まれており、かつCAサブシステム350はコンテンツ鍵を取り出す。CAサブシステムはコンテンツ鍵を使用して、デクリプタ360により行われる暗号化されたデータの復号化を制御する。デクリプタ360は、通常、デスクランブラと称される。セキュリティのために、制御ワードは、頻繁に（例えば、特定の時間期間の後またはある量のデータの伝送後に）変更される。新たなECMは、制御ワードの値を毎回変更して受信器へ転送しなければならない。したがって、条件付きアクセスが可能なデータ・サービスの各々には、ECMストリームが関連付けられる。変更されていないECMを数回再伝送して、受信器がサービスに

アクセスするためにかかる時間を低減させることが必要となる場合がある（サービスにアクセスするために、受信器は対応するECMを最初に取得しなければならない）。本発明の場合、幾つのセキュリティ・レイヤが用いられているかということは問題とされない。本発明は、複数の制御ワード・ストリームの処理を扱っており、関連付けられている復号化されたコンテンツ鍵がデスクランブラに供給される。（例えば1つ以上の中間的な暗号化レイヤを介した）制御ワード間の厳密な関係が本発明に影響を及ぼすことはない。様々な異なるセキュリティ・レイヤを有するシステムにも本発明を適用することが当業者に可能となるであろう。本システムが、MPEGコーディング、およびDVBのようなアーキテクチャを一例として用いて説明されていることも認識されるであろう。複数のスクランブル化されたストリームが多重化された形態で伝送される他のシステム内でも、本発明を活用することができる。

【００１８】

このようなスキームが稼動するためには、受信器は権限鍵への安全なアクセスを得る必要がある。このためには通常、たいていスマートカード内に組み込まれた固定された1つのデバイス鍵が各デバイスに関連付けられる。伝送器は、固定された全てのデバイス鍵へのアクセス権を持つ。伝送器はデバイスに関連付けられている固定されたデバイス鍵をデバイス毎に取り出し、かつエンクリプタ320を使用して、固定されたデバイス鍵の制御下で権限鍵を暗号化する。暗号化された権限鍵は、次に、いわゆる資格管理メッセージ（EMM: Entitlement Management Message）を用いて、関連付けられている受信器だけに伝送される。このことは、各受信器に一意の識別子を与えかつこの識別子をEMM内のアドレスとして使用することにより実現される。EMMをブロードキャストすると、各受信器はEMMを受信する。但し、このアドレスに識別子がマッチングする受信器だけが、EMMを受信し、かつ権限鍵を復号化する。受信器にはデクリプタ380が含まれている。デクリプタ380は、固定されたデバイス鍵の制御下で使用されて、受信された暗号化されている権限鍵を復号化する。取り出された権限鍵は、次に、デクリプタ370を制御するために用いられる。残り部分に関しては、デクリプタ370と380の役割を集合的に「デクリプタ」と称する。デクリプタは、デバイス鍵を保持するスマートカード内にも組み込むことが好ましい。

【００１９】

図4は、ブロードキャスト受信器の処理態様の更なる詳細を示している。ブロードキャスト受信器には、チューナ機能410、デマルチプレクサ機能420、デスクランブラ機能430、デクリプタ機能440、およびデコーダ機能450が含まれている。これらの機能は、専用ハードウエアを使用して行うことができる。これらの機能の幾つか、つまり一部を、（例えば、適切なプログラムがロードされているデジタル信号処理プロセッサ（DSP）を用いて）プログラム可能なプロセシング機能により行ってもよい。デスクランブラとデクリプタは、共に、条件付きアクセス・システムの中心部分を形成する。受信器内の様々な機能は、埋め込み型のマイクロプロセッサまたはマイクロ制御器が通常含まれている制御器460の制御下で動作する。図面を簡素に保つために、制御器と他の機能との間の制御関係は、図示されていない。制御器が制御ワードとコンテンツ鍵を処理する際に有することができる役割しか、図示されていない。ユーザ・インタフェース470により、受信器はユーザと相互作用することができる。ユーザ・インタフェース470には、IR遠隔制御器から信号を受信するための赤外線受信器、キーボード、または音声制御を行うためのマイクロホンなどの、いかなる適切なユーザ入力手段を含めてもよい。出力には、小型のLCD表示装置を使用すること、またはテレビジョン表示装置を使用すること、または更には可聴フィードバックなどのいかなる適切な形態を用いてもよい。通常動作の間、ユーザは、チャネル／サービスを選択する。この選択は、通常、ユーザがユーザ・インタフェース470を使用して、プリセットされている数を指示することにより行われる。このプリセットされている数は、メモリ480内に格納されている、組み込まれている全てのチャネルを有するテーブルを用いて、チューナ410とデマルチプレクサ420の制御に適した形態に翻訳される。デジタル・システムの場合、この形態は、network_id、transport_stream_id、およびchannel_idなどのチャネル識別とすることができる。デジタル・ストリーム内で伝送されるネッ

トワーク情報テーブル（NIT）使いてtransport_stream_idを周波数に翻訳すると、チューナ410は、周波数多重化されたトランスポート・ストリームにチューニングすることが可能となる。チャネルIDにより、デマルチプレクサは、多重化されたストリームから所望のチャネルを抽出することができる。チャネルがスクランブル化されている場合、チャネルは、デスクランブラ430を通してフィードされ、かつ次にデコーダ450を通してフィードされる。プレーンなストリームは、デスクランブラをバイパスして、デコーダに直接供給することができる。デコーダの出力は、レンダリング・デバイスまたは格納デバイスに供給して、後でレンダリングすることができる。特定のアプリケーションの場合、受信器は、エンコードされた出力ストリームを、デコーダ450をバイパスさせて提供してもよい。その後レンダリング・デバイスにデコーダ機能を含めたり、またはエンコードされたストリームを後の段階で受信器に再供給して、更なるデコーディングを行ってもよい。同様に、スクランブル化されているストリームを、このストリームを最初にデスクランブル化せずに、スクランブル化されている形態で格納することが原則的に可能である。このストリームは、後でデスクランブラを通してフィードすることにより、後の段階でデスクランブル化することができる。制御ワード・ストリームは、原則としてデータ・ストリームと並列に走るので、この場合、両方のストリームを同期化させるには特別な注意が必要である。説明を単純化すると、残り部分では、受信器はデータ・ストリームを一度で完全に処理することが仮定されている。但し、本発明の原理を他の状況にも適用することが当業者には可能となるであろう。

【００２０】

本発明によると、デマルチプレクサは、少なくとも2つのデータ・ストリームに対して制御ワード・ストリームを供給する。実際には、デマルチプレクサはこれらのデータ・ストリームをこのときに全て提供してもよいが、受信器の残り部分がこれらのデータ・ストリームを使い果たす必要はない。デマルチプレクサにより供給される制御ワード・ストリームが、周波数多重化された同一のトランスポート・ストリーム内で利用可能な場合、1つのトランスポート・ストリームへのチューニングしかサポートしないチューナ機能を用いてもよい。複数の独立したトランスポート・ストリームへのチューニングが可能なチューニング機能を用いることが好ましい。このために、1つのトランスポート・ストリームへのチューニングが各々可能な幾つかの並列に構成されたチューニング・ユニットをチューナ410に含めてもよい。同様に、デマルチプレクサ機能420が、非多重化を行う一組のハードウエア／ソフトウエアを使用したり、または並列構成された複数の組を使用して、複数の制御ワード・ストリームを提供できるようにしてもよい。制御ワード・ストリームは、周波数が相対的に低い。例えば、関連付けられているデータ・ストリームのための新たな制御ワードを有するECMを10秒毎に供給してもよい。EMMは、通常、均一なはるかに低いレートで供給される。通常このストリームは、周波数が低いので、受信器の主制御器460により管理される。適切な制御ワードが受信器内に存在しなければ、復号化とデスクランブル化が開始できないことが理解されるであろう。従来は、最初にユーザがチャネルを選択し、次にチューナとデマルチプレクサを制御して、チャネルと関連付けられている制御ワード・ストリームとを供給しなければならなかった。制御ワードが一度受信されたら、最初にこの制御ワードを復号化することが必要で、このときに初めてデスクランブル化が開始可能となった。この従来のシステムにおける第一制御ワードの受信待ち時間を低減させるためには通常、同一の制御ワードが繰り返し（例えば、10秒毎に）ブロードキャストされる。一連の幾つかの同一の制御ワードの内1つだけを復号化すればよいので、制御器は、複製コピーを削除することにより、制御ワード・ストリームをフィルタリングすることができる。制御器は、制御ワードのフィルタリングされたストリームをデクリプタ440にフィードする。デクリプタは、復号化された制御ワード（すなわち、コンテンツ鍵）を制御器460に供給し戻す。全てのデータ・ストリーム、およびこれらに対応する制御ワードのストリームを原則的に非同期にして、制御ワードの周波数と、制御ワードの供給の瞬間とを互いに独立させてもよい点に留意すべきである。このような非同期的挙動を扱うために、幾つかの独立した制御ワード・ストリームを処理することができる特殊なデクリプ

タを用いてもよい。

【００２１】

好ましい一実施例では、制御ワードのストリームを1つしか処理しないように設計されている従来のデクリプタが使用される。この場合、制御器がデクリプタに制御ワードを供給し、デクリプタが制御ワードを（例えば、300～600 m秒で）復号化し、かつコンテンツ鍵を供給し返す。デクリプタは、制御ワードを復号化している間、他の制御ワードを復号化することはできないが、1つのストリームしかデスクランブル化されない従来のシステムの場合は通常、このような制御ワードがこのような期間内に到着することはない。このため、従来のこのようなデクリプタは、複数の非同期制御ワード・ストリームを処理することに適していない。本発明によると、制御器460は、非同期の制御ワード・ストリームを同期化させ、かつ多重化された1つの制御ワード・ストリームをデクリプタに提供する。図5には、このことが示されている。この図中、制御ワードの3つの独立したストリーム510、520、530が、制御器460のフィルタリング機能540を通してフィードされている。フィルタの出力は、待ち行列として作用する1つのバッファ550内に入れられる。図4のメモリ480を用いて、この待ち行列を格納してもよい。制御ワードは、通常、到着した時間シーケンスで待ち行列内に入れられる。制御器は、制御ワードを待ち行列内の到着シーケンスで待ち行列からデクリプタ560に供給する。制御器は、デクリプタが前に供給された制御ワードの処理でまだビジー状態のままか否かをモニタする。デクリプタがビジー状態である限り、新たなワードは供給されない。デクリプタがフリー状態になると直ぐに、新たなワードを（このようなワードが既に待ち行列内に存在している場合）供給することができる。制御器は、デクリプタにより供給されたコンテンツ鍵をメモリ内に確実に格納する。活性データ・ストリームの場合、コンテンツ鍵は、デスクランブラに直ちに供給してもよいし、またはトリガがブロードキャスト信号を介して与えられ、現在到着しているデータが、次のコンテンツ鍵によりスクランブル化されるようになる時点まで保持してもよい。コンテンツ鍵は、デスクランブラにより実際に使用されるまで、受信器の汎用メモリ内に格納しておいてもよい。望ましい場合、コンテンツ鍵を、デスクランブラ内の専用レジスタ内に予め格納しておいて、より高速なスイッチングを可能にしてもよい。デスクランブラがまだ処理していないデータ・ストリームの場合、制御器はコンテンツ鍵を汎用メモリ内に格納して、このデータ・ストリームが更なる処理のために選択されかつデスクランブラに供給されたとき、デスクランブラに「即時に」供給できるようにしておくことが好ましい。デスクランブラへのデータ・ストリームの供給と対応するコンテンツ鍵とは、このとき同期化される。図5には、図示されている各制御ワード・ストリーム510、520、530毎に、1つのコンテンツ鍵570、580、590が格納されることが示されている。

【００２２】

従来は、奇数の制御ワードと偶数の制御ワードとたいてい称される2つの制御ワードが、データ・ストリームに対して「活性化」されていた。これらの制御ワードの内の1つに対応するコンテンツ鍵を用いてデータ・ストリームの現在の部分をデスクランブル化している間に、次の制御ワードは、全ての受信器に早くもブロードキャストされる。このことにより、受信器は第二制御ワードを復号化することができる。ブロードキャスト・ストリーム内の指示に追従して、デスクランブル化は新たな鍵にスイッチされる。本発明による受信器の場合、上述したように、本システムにより処理された制御ワード・ストリーム毎に2つのコンテンツ鍵が格納される。このことを、鍵を3つ以上格納する必要がある他のシステムに適合化させることが、当業者には可能となるであろう。

【００２３】

好ましい一実施例の場合、格納されている復号化された制御ワードを用いて、新たなチャネルを速く選択することが可能となる。例えば、ユーザは、ビューイング（または格納）のためのチャネルを1つ選択している場合がある。制御器は、ユーザが次に選択したい可能性があるチャネルを1つ以上推定する。制御器は、チューナ／デマルチプレクサに命令して、この予測されたチャネルに対する制御ワード・ストリームを早くも供給する。上述したように、制御器は、これらの予測されたチャネル毎に少なくとも1つのコンテンツ

鍵を利用可能にさせる。実際に新たなチャネルが選択されたら、この新たに選択されたストリーム用の制御ワードの受信を待機してかつこの制御ワードを復号化することを最初に行わなくても、対応するデータ・ストリームをデスクランブラに供給して、コンテンツ鍵を供給することが直ちに可能となる。通常は、制御ワードを到着時間シーケンスで待ち行列550内に入れてもよいが、ユーザが新たなチャネルを選択したときには、新たなストリームの制御ワードを必ず優先させることが好ましい。例えば、ユーザがチャネル10を選択した場合、このチャネルが正確に予測されていれば、このチャネル用のコンテンツ鍵は準備ができているはずである。新たに予測されたチャネルは、チャネル11としてもよい。この場合、制御器によって、チャネル11用の制御ワードがデマルチプレクサにより確実に供給される。利用可能なコンテンツ鍵の寿命がまだ十分残されている場合、制御器はデクリプタが利用可能になったら直ちに、チャネル11用の第一受信制御ワードをデクリプタに提供することが好ましい。このことは、デクリプタに次に出力される場所に制御ワードを挿入することにより行うことができる。

【００２４】

予測されたストリーム毎に、大きなパケットもフィルタリング除去して、デコーディングの遅延を低減させることが好ましい。例えば、MPEGコード化されたストリームのデコーディングの場合、フレームのデコーディングには、少なくとも（フレーム内コード化された）Iフレームが存在している必要がある。1つ以上のフレームを格納することにより、デコーディング時の待ち時間を減少させることができる。

【００２５】

チャネルの予測は、いかなる適切な形態で行ってもよい。例えば、予測アルゴリズムは、視聴者がザッピング動作を行っていると仮定することに基づくことができる。ユーザが上方向へザッピングしている（つまり、プリセット3がプリセット2の後に選択される）場合、次のチャネルが同じ上方にある（つまり、プリセット4）と仮定することが妥当である。この例では、プリセット番号とは格納されているプリセットの数のことであり、必ずしも下にあるチャネルの数のことではない。受信器が持っている容量が、追加的な制御ワード・ストリームを1つしか処理できない場合、予測されるプリセットは、ザッピング方向にある次のプリセット番号となる。次に、このプリセットに対応するチャネル用の制御ワード・ストリームがロードされる。受信器が持っている容量が、追加的な制御ストリームを2つ処理できる場合、次のプリセットと前のプリセットを予測されるプリセットにして、ザッピング方向を変えるユーザに対応するようにしてもよい。例えば、ユーザが、主に、例えば、スポーツ番組、ニュース番組などの特定分類の番組範囲内のプリセットをザッピングすると仮定する、より高度なアルゴリズムを更に用いてもよい。隠れマルコフ・モデルなどの統計アルゴリズムを用いて、ユーザの行動を知りかつ予測してもよい。

【００２６】

別の好ましい実施例の場合、本発明による技法を用いて、複数のデータ・ストリームを「同時に」デスクランブル化する。デスクランブラが時間多重化による手法で動作すること、すなわち、1つのストリームを処理することができるハードウエア／ソフトウエアをより高い周波数で動作させることによって、2つ以上のストリームが処理可能となることは有利である。このとき制御器により、2つ以上の入力データ・ストリームの間で処理が、規則的な間隔で確実にスイッチされる。処理がスイッチされる毎に、新たなストリーム用のコンテンツ鍵もデスクランブラにロードされる。デマルチプレクサは、選択されたデータ・ストリームを、時間多重化による手法でその出力へ提供することが好ましい。これに代えて、デマルチプレクサは、その出力に、2つ以上の並列なデータ・ストリームを各々通常のタイミングで提供してもよい。この場合、制御器は、これらの複数の出力ストリームを、時間多重化された1つのストリームに組み合わせることが好ましい。このことは、データ・ストリームの内の1つから（例えば、100 m秒の信号に対応する）1ブロックを交互にコピーし、かつこのコピーをデスクランブラに提供する（つまり、FIFOバッファ内にコピーして後でデスクランブラへ供給する）ことにより行うことができる。このことが3つの並列ストリームで発生する場合、デスクランブラは、各々、100 m秒のデータ片を少

なくとも1/3×100 m秒内にデスクランブル化して、スイッチング・オーバーヘッドのためにある程度の余地を残しておくことが可能でなければならない。

【００２７】

上述の実施例は、本発明を限定ではなく例示しているのであり、かつ添付の請求の範囲の範囲内で多数の代替実施例を設計することが当業者には可能となるであろうことに留意すべきである。請求項では、括弧の間に配置された何れの引用符号も、請求項を限定するものと解釈してはならない。「有する」および「含む」という語は、請求項に列挙されている要素またはステップ以外のものを除外するわけではない。本発明は、幾つかの別個要素を有するハードウエアにより、かつ適切にプログラムされたコンピュータにより実施可能である。システム／デバイス／装置に関する請求項には幾つかの手段が列挙されているが、これらの手段の幾つかは、全く同一のハードウエア品目により具現化することができる。コンピュータ・プログラム製品は、光学格納装置などの適切な媒体上へ格納／配信させることができるが、インターネットまたはワイヤレス通信システムを介した配信などの他の形態で配信してもよい。

【図面の簡単な説明】

【００２８】

【図１】本発明を用いることができるデジタル・ブロードキャスト・システムのブロック図を示す。

【図２】本システム内で用いるためのブロードキャスト受信器のブロック図を示す。

【図３】制御ワードとコンテンツ鍵の例示的な使用法を示す。

【図４】ブロードキャスト受信器の処理構造の詳細を示す。

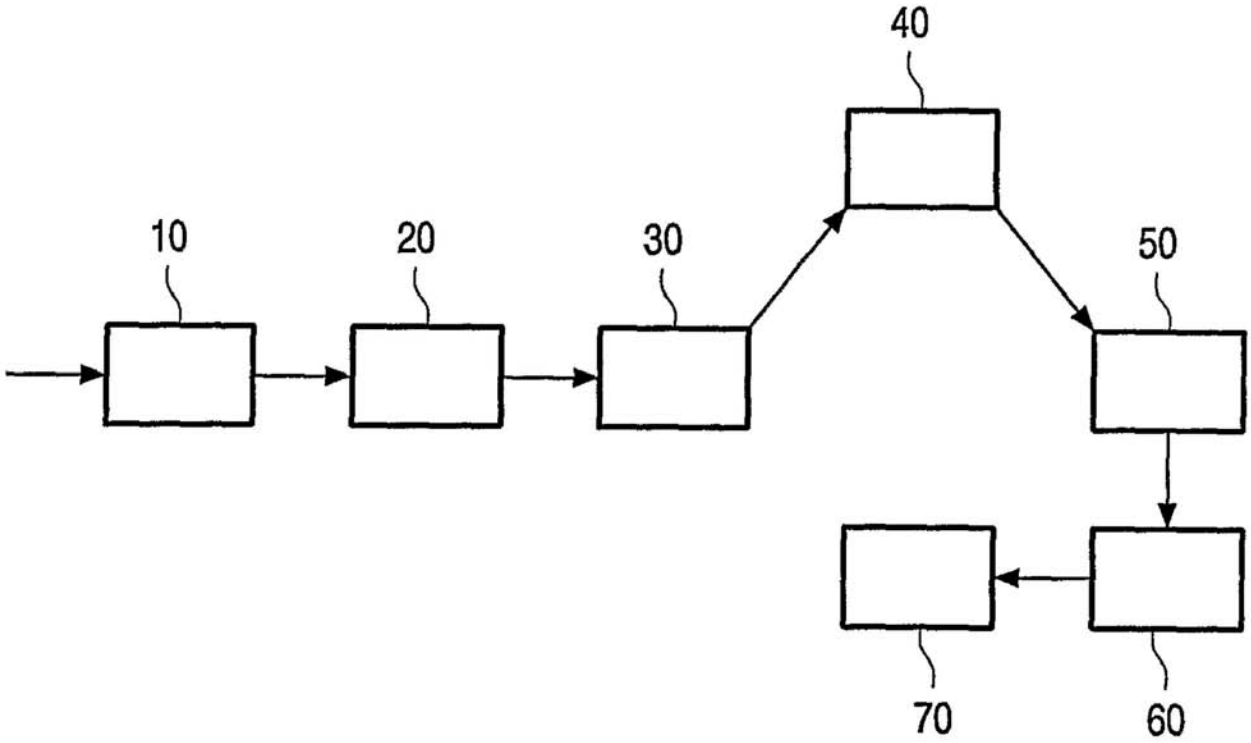
【図５】制御ワードとコンテンツ鍵の流れと格納装置を示す。

【符号の説明】

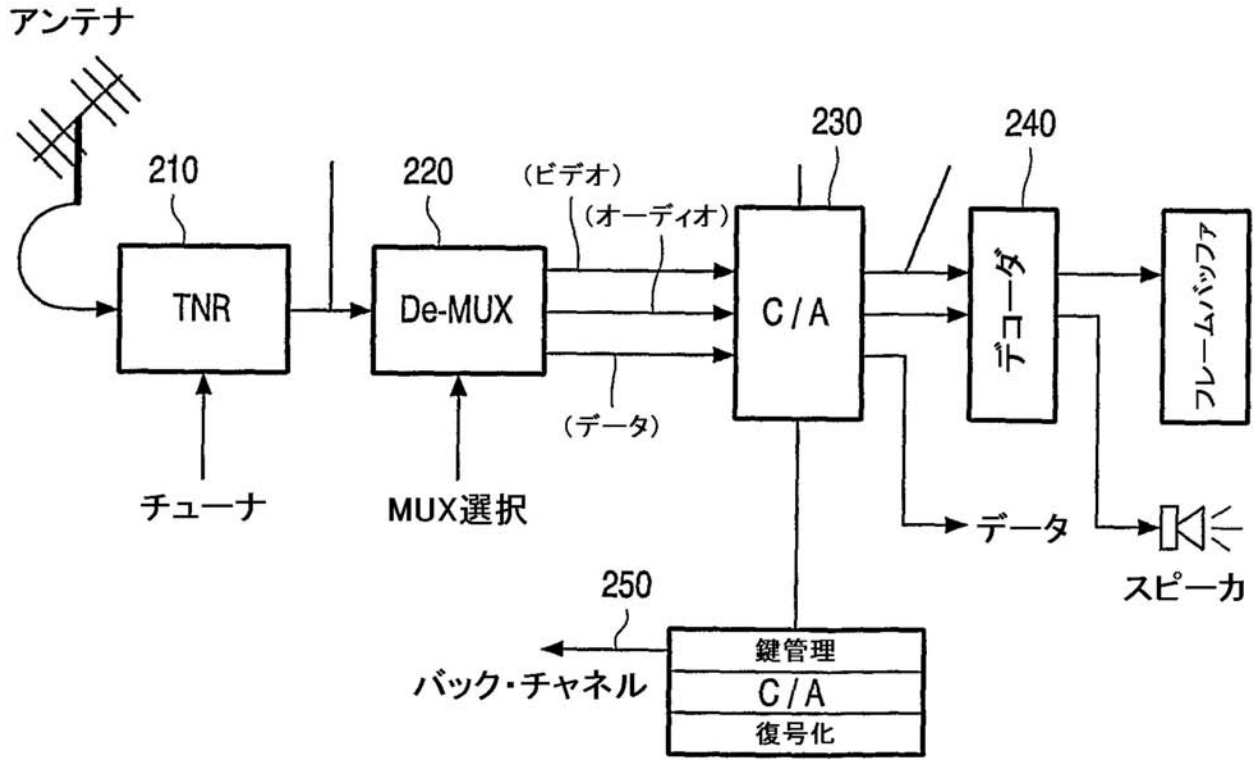
【００２９】

410…チューナ
420…デマルチプレクサ
430…デスクランブラ
450…デクリプタ
460…制御器
510…制御ワード・ストリーム
520…制御ワード・ストリーム
530…制御ワード・ストリーム
550…制御ワード
560…デクリプタ
570…コンテンツ鍵ストリーム
580…コンテンツ鍵ストリーム
590…コンテンツ鍵ストリーム

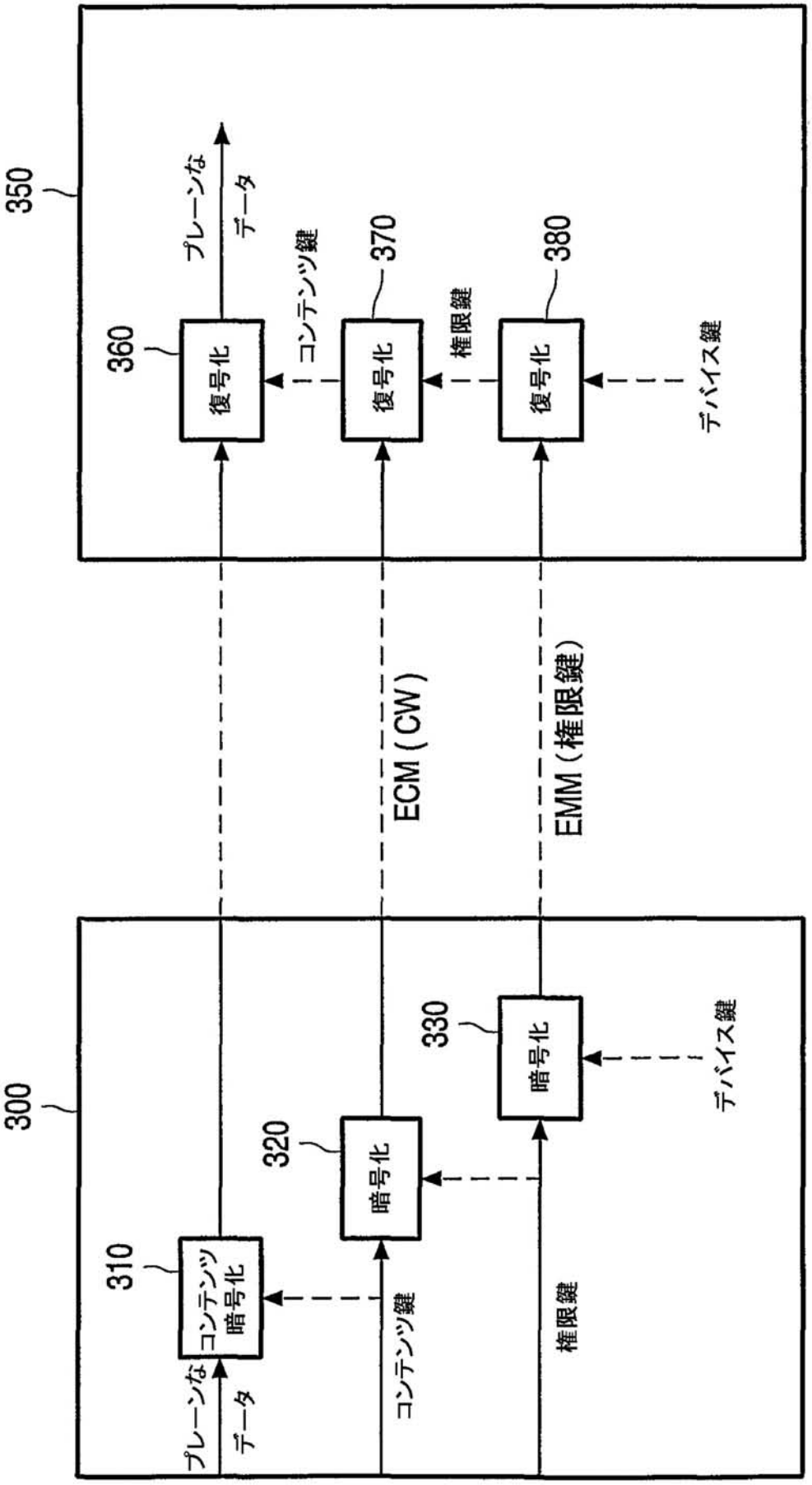
【図１】


40
10
20
30
50
70
60

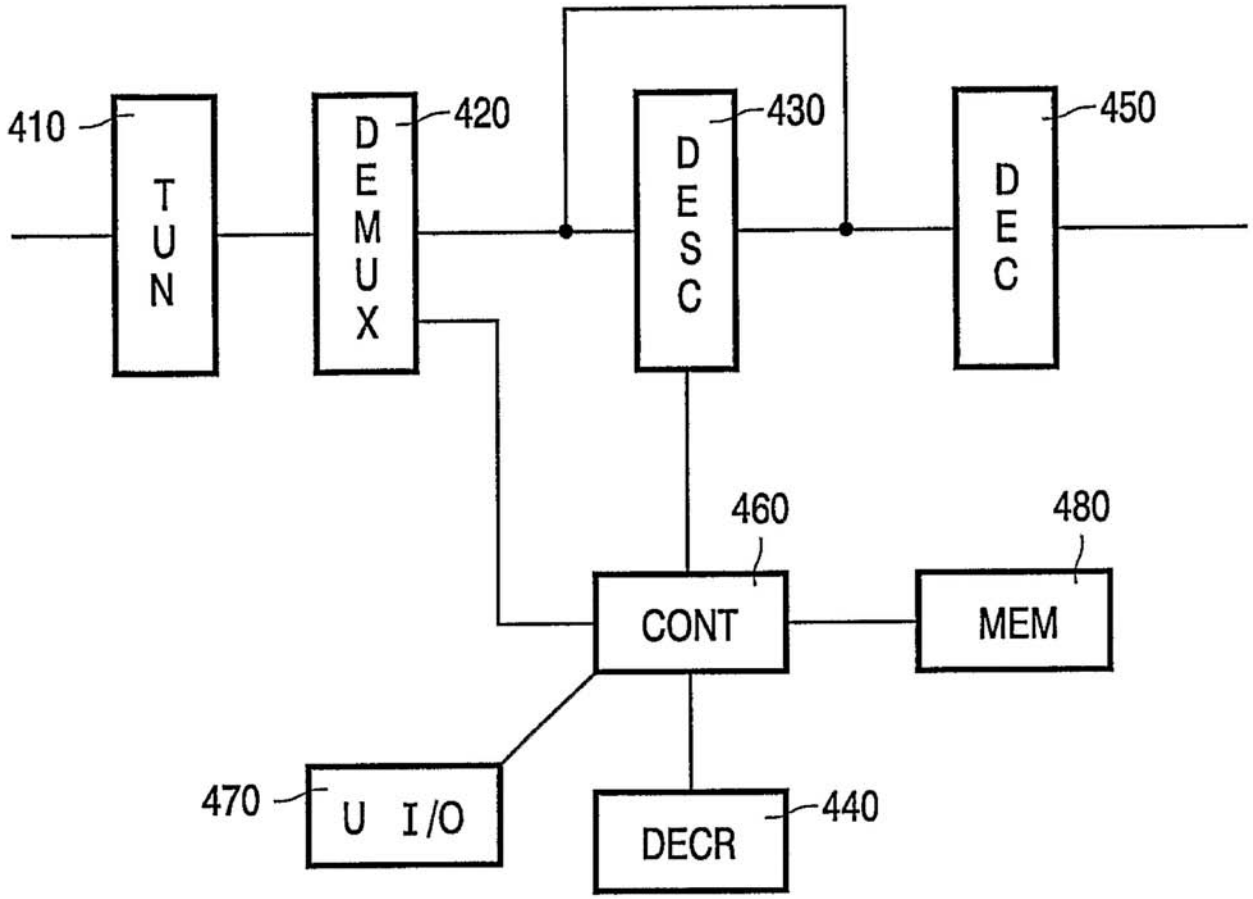
【図２】


アンテナ
210
220
(ビデオ)
(オーディオ)
230
240
TNR
De-MUX
C/A
デコーダ
フレームバッファ
(データ)
チューナ
MUX選択
データ
スピーカ
250
鍵管理
C/A
復号化
バック・チャネル

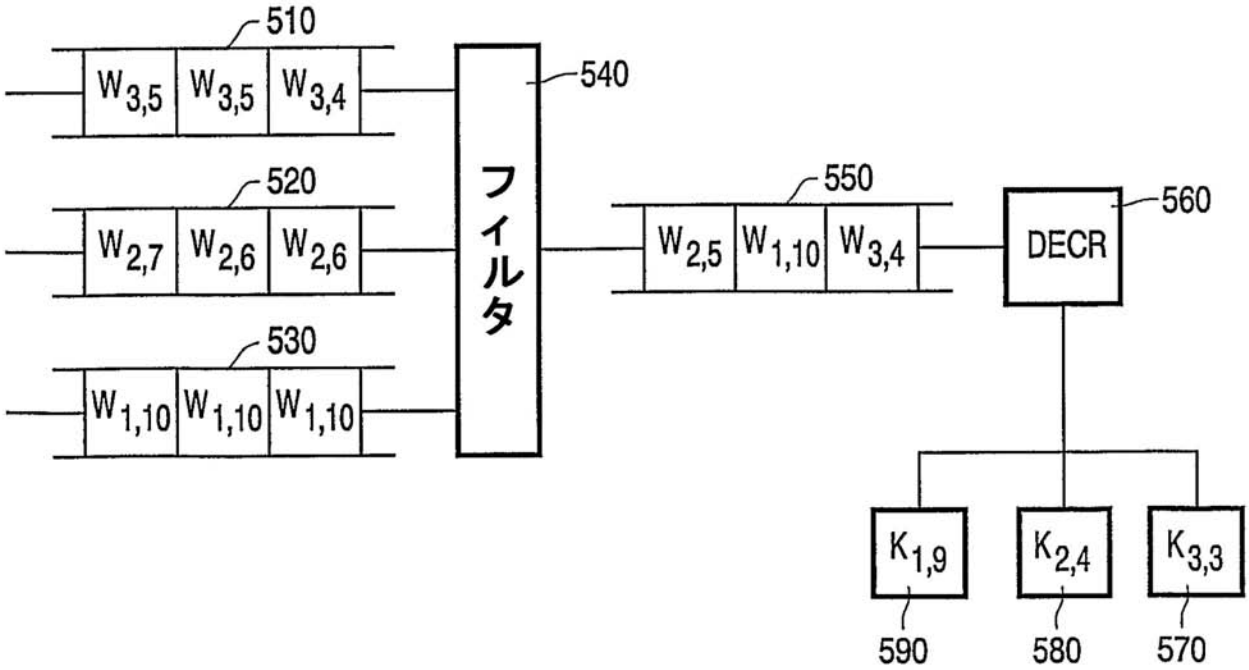
【図３】


300
310
コンテンツ暗号化
プレーンなデータ
コンテンツ鍵
320
暗号化
330
暗号化
権限鍵
デバイス鍵
ECM (CW)
EMM (権限鍵)
350
360
復号化
プレーンなデータ
コンテンツ鍵
370
復号化
権限鍵
380
復号化
デバイス鍵

【図４】


410
TUN
DEMUX
420
DESC
430
DEC
450
460
CONT
480
MEM
470
U I/O
DECR
440

【図５】


510
W3,5
W3,5
W3,4
520
W2,7
W2,6
W2,6
530
W1,10
W1,10
W1,10
フィルタ
540
550
W2,5
W1,10
W3,4
DECR
560
K1,9
K2,4
K3,3
590
580
570

【国際調査報告】

INTERNATIONAL SEARCH REPORT

PCT/IB 03/01713

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/00 H04N7/16

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)
IPC 7 H04N

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 982 935 A (CSELT CENTRO STUDI LAB TELECOM) 1 March 2000 (2000-03-01) page 3, column 4, line 9 -page 5, column 7, line 52 figures 1-3	1-6
Y	WO 99 16247 A (SARNOFF CORP) 1 April 1999 (1999-04-01) page 5, line 4 -page 17, line 3 figures 1-3	1-6
A	BANKS D ET AL: "BREAKING OPEN THE SET TOP BOX" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 3228, 4 November 1997 (1997-11-04), pages 105-116, XP002064906	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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
29 July 2003	06/08/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

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

INTERNATIONAL SEARCH REPORT

on patent family members

PCT/IB 03/01713

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0982935 A	01-03-2000	IT T0980705 A1	11-02-2000
		EP 0982935 A2	01-03-2000
		JP 2000115748 A	21-04-2000
WO 9916247 A	01-04-1999	US 6118498 A	12-09-2000
		AU 9585498 A	12-04-1999
		AU 9588198 A	12-04-1999
		AU 9588298 A	12-04-1999
		AU 9670698 A	12-04-1999
		AU 9778898 A	12-04-1999
		CN 1302506 T	04-07-2001
		CN 1299562 T	13-06-2001
		EP 1025537 A1	09-08-2000
		EP 1025709 A1	09-08-2000
		EP 1025697 A1	09-08-2000
		EP 1055325 A1	29-11-2000
		EP 1025692 A2	09-08-2000
		JP 2001517879 T	09-10-2001
		JP 2002517109 T	11-06-2002
		JP 2001517904 T	09-10-2001
		JP 2001517906 T	09-10-2001
		US 5933195 A	03-08-1999
		US 6122400 A	19-09-2000
		US 6057889 A	02-05-2000
		US 6118486 A	12-09-2000
		US 5987180 A	16-11-1999
		WO 9916011 A1	01-04-1999
		WO 9916243 A1	01-04-1999
		WO 9916242 A1	01-04-1999
		WO 9916012 A1	01-04-1999
		WO 9916253 A1	01-04-1999
		WO 9916247 A1	01-04-1999
		WO 9916235 A2	01-04-1999
		US 2002176506 A1	28-11-2002
		US 6549240 B1	15-04-2003

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ヴァン デア ハイユデン
オランダ国 ５６５６ アー アー アインドーフェン プロフホルストラーン ６
(72)発明者 ゲラルダス, ヴェー. , テー.
オランダ国 ５６５６ アー アー アインドーフェン プロフホルストラーン ６

Ｆターム(参考) 5C025 AA30
5C064 CA14 CB01 CC01 CC04

【要約の続き】
450、560に制御ワード550を供給する。デクリプタはこれらの制御ワードを復号化し、かつ対応するコンテンツ鍵を制御器に供給する。制御器は、制御ワード・ストリーム毎に、対応するコンテンツ鍵ストリーム570、580、590を形成し、かつコンテンツ鍵ストリーム毎に少なくとも１つの最新のコンテンツ鍵をメモリ内に格納する。制御器が、選択された非多重化されたデータ・ストリームに対して、対応するコンテンツ鍵をメモリからデスクランブラに提供すると、デスクランブラはデータ・ストリームをデスクランブル化することが可能となる。