

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2010-51032
(P2010-51032A)

(43) 公開日 平成22年3月4日(2010.3.4)

(5) Int.Cl.	F I	テーマコード (参考)
HO4N 7/167 (2006.01)	HO4N 7/167 Z	5C164
HO4N 7/173 (2006.01)	HO4N 7/173 610Z	5J104
HO4L 9/14 (2006.01)	HO4L 9/00 641	

審査請求 有 請求項の数 8 O L (全 90 頁)

(2) 出願番号 特願2009-273566 (P2009-273566)
 (22) 出願日 平成21年12月1日 (2009.12.1)
 (62) 分割の表示 特願2003-561245 (P2003-561245) の分割
 原出願日 平成14年12月13日 (2002.12.13)
 (31) 優先権主張番号 10/037,499
 (32) 優先日 平成14年1月2日 (2002.1.2)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 2,405,899
 (32) 優先日 平成14年10月1日 (2002.10.1)
 (33) 優先権主張国 カナダ (CA)

(71) 出願人 593181638
 ソニー エレクトロニクス インク
 アメリカ合衆国 ニュージャージー州 O
 7656 パークリッジ ソニー ドライ
 ブ 1
 (71) 出願人 000002185
 ソニー株式会社
 東京都港区港南1丁目7番1号
 (74) 代理人 100082005
 弁理士 熊倉 禎男
 (74) 代理人 100067013
 弁理士 大塚 文昭
 (74) 代理人 100109070
 弁理士 須田 洋之

最終頁に続く

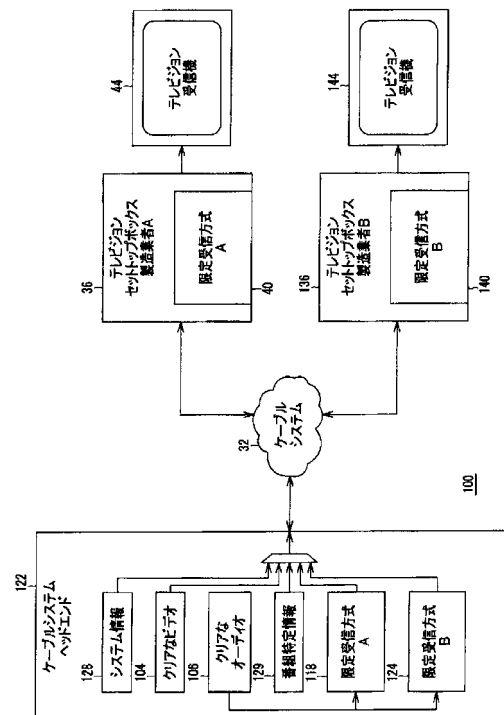
(54) 【発明の名称】 部分暗号化及びパケット識別子のマッピング

(57) 【要約】

【課題】 テレビジョン番組を複数の方式で暗号化する暗号化構成を提供する。

【解決手段】 本発明に基づくシステムは、テレビジョン番組を完全に表現するために必要なデータの一部のみを複数の方式で暗号化し、これにより、単一のシステム内で、複数の製造業者のセットトップボックス(36、136)に関連する複数の限定受信方式(40、140)を共存させることができるようになる。複数の暗号化方式間を区別するために、PIDマッピング技術を用いる。番組の一部のみを暗号化することにより、全ての番組データを複数の方式で暗号化した場合に比べて、消費される帯域幅を著しく削減することができ、これにより、単一のケーブルテレビジョンシステム(32)において、多数の限定受信方式を同時に用いることができる。

【選択図】 図2



【特許請求の範囲】

【請求項 1】

第 1 の暗号化法に基づいて暗号化されているテレビジョン番組の複数の暗号化されたサンプルと、

暗号化されていない部分とを有する暗号化されたテレビジョン信号。

【請求項 2】

当該テレビジョン信号は、デジタルテレビジョン信号であり、上記暗号化されたサンプルは、暗号化されたパケットを含み、上記暗号化されていない部分は、暗号化されていないパケットを含むことを特徴とする請求項 1 記載の暗号化されたテレビジョン信号。

【請求項 3】

上記デジタルテレビジョン信号は、MPEG規格に準拠し、上記暗号化されたパケットは、パケット識別子によって識別されることを特徴とする請求項 2 記載の暗号化されたテレビジョン信号。

【請求項 4】

上記デジタルテレビジョン信号は、MPEG規格に準拠し、上記暗号化されていないパケットは、第 1 のパケット識別子によって識別され、上記暗号化されたパケットは、該第 1 のパケット識別子によって識別されることを特徴とする請求項 2 記載の暗号化されたテレビジョン信号。

【請求項 5】

上記デジタルテレビジョン信号は、MPEG規格に準拠し、上記暗号化されていないパケットは、第 1 のパケット識別子によって識別され、上記暗号化されたパケットは、第 2 のパケット識別子によって識別されることを特徴とする請求項 2 記載の暗号化されたテレビジョン信号。

【請求項 6】

複数の暗号化されていないパケットと、

複数の暗号化されたパケットとを含み、

上記暗号化されていないパケット及び暗号化されたパケットは、いずれも当該テレビジョン番組データをデコードするために必要とされる暗号化されたテレビジョン番組データ

【請求項 7】

上記暗号化されていないパケット及び暗号化されたパケットは、トランスポートストリームパケットを含むことを特徴とする請求項 6 記載の暗号化されたテレビジョン番組データ。

【請求項 8】

上記デジタルテレビジョン信号は、MPEG規格に準拠し、上記暗号化されたパケット及び暗号化されていないパケットは、パケット識別子によって識別されることを特徴とする請求項 6 記載の暗号化されたテレビジョン番組データ。

【請求項 9】

上記デジタルテレビジョン信号は、MPEG規格に準拠し、上記暗号化されていないパケットは、第 1 のパケット識別子によって識別され、上記暗号化されたパケットは、第 2 のパケット識別子によって識別されることを特徴とする請求項 6 記載の暗号化されたテレビジョン番組データ。

【請求項 10】

コンテンツを暗号化する暗号化方法において、

上記コンテンツの 100%未満を暗号化する選択アルゴリズムに基づいて暗号化するべきコンテンツの部分を特定するステップと、

上記特定されたコンテンツの部分を第 1 の暗号化法に基づいて暗号化し、第 1 の暗号化された部分を生成するステップと、

上記特定されたコンテンツの部分を第 2 の暗号化法に基づいて暗号化し、第 2 の暗号化された部分を生成するステップと、

10

20

30

40

50

暗号化されていない部分とともに、上記第 1 の暗号化された部分と、第 2 の暗号化された部分とを結合し、デュアル部分暗号化されたコンテンツを生成するステップとを有する暗号化方法。

【請求項 1 1】

上記第 1 の暗号化された部分と、上記第 2 の暗号化された部分とを結合し、デュアル部分暗号化されたコンテンツを生成するステップを更に有する請求項 1 0 記載の暗号化方法。

【請求項 1 2】

上記暗号化されていない部分を上記第 1 の暗号化された部分と、上記第 2 の暗号化された部分とともに配信するステップを更に有する請求項 1 0 記載の暗号化方法。

10

【請求項 1 3】

上記コンテンツは、テレビジョン信号を含み、上記デュアル部分暗号化されたコンテンツは、デュアル部分暗号化されたテレビジョン信号を含むことを特徴とする請求項 1 0 記載の暗号化方法。

【請求項 1 4】

ケーブルシステム、地上波放送システム、衛星システム、パッケージ媒体のいずれかを介して、上記デュアル部分暗号化されたテレビジョン信号を配信するステップを更に有する請求項 1 3 記載の暗号化方法。

【請求項 1 5】

上記テレビジョン信号は、オーディオ部分、ビデオ部分及びシステム情報部分を有することを特徴とする請求項 1 3 記載の暗号化方法。

20

【請求項 1 6】

上記選択アルゴリズムは、暗号化のために上記システム情報部分を選択することを特徴とする請求項 1 5 記載の暗号化方法。

【請求項 1 7】

上記選択アルゴリズムは、暗号化のために上記オーディオ部分を選択することを特徴とする請求項 1 5 記載の暗号化方法。

【請求項 1 8】

上記選択アルゴリズムは、暗号化のために上記ビデオ部分を選択することを特徴とする請求項 1 5 記載の暗号化方法。

30

【請求項 1 9】

上記コンテンツは、複数のプログラムを有し、上記選択アルゴリズムは、暗号化のために、所定の期間、各プログラムを連続的に選択することを特徴とする請求項 1 0 記載の暗号化方法。

【請求項 2 0】

上記コンテンツは、複数のプログラムを有し、上記選択アルゴリズムは、暗号化のために、所定の期間、100%未満の各プログラムを連続的に選択することを特徴とする請求項 1 0 記載の暗号化方法。

【請求項 2 1】

上記コンテンツは、データのブロックを含み、MをNより大きい数として、上記選択アルゴリズムは、暗号化のために、各M個のブロック毎にN個のブロックを選択することを特徴とする請求項 1 0 記載の暗号化方法。

40

【請求項 2 2】

上記コンテンツは、データ構造を有し、上記選択アルゴリズムは、暗号化のために、該データ構造の断片を選択することを特徴とする請求項 1 0 記載の暗号化方法。

【請求項 2 3】

上記コンテンツは、圧縮データを含み、上記選択アルゴリズムは、暗号化のために該コンテンツを伸張するために必要なデータを選択することを特徴とする請求項 1 0 記載の暗号化方法。

【請求項 2 4】

50

上記コンテンツは、複数のエレメンタリストリームパケットを含み、上記選択アルゴリズムは、暗号化のために、ヘッダ情報を選択することを特徴とする請求項 10 記載の暗号化方法。

【請求項 25】

上記ヘッダ情報は、パケット化エレメンタリストリーム (P E S) ヘッダ、シーケンスヘッダ、シーケンスヘッダエクステンション、グループオブピクチャ (G O P) ヘッダのうち少なくとも 1 つを含む請求項 24 記載の暗号化方法。

【請求項 26】

上記コンテンツは、第 1 のパケット識別子 (P I D) を用いてパケット化され、暗号化のために選択されるコンテンツを含むパケットの P I D は、第 2 の P I D にマッピングされることを特徴とする請求項 10 記載の暗号化方法。

10

【請求項 27】

暗号化されていないコンテンツ部分を第 1 及び第 2 の暗号化されたコンテンツ部分とは別に配信するステップを更に有する請求項 10 記載の暗号化方法。

【請求項 28】

プログラミングされたプロセッサによって実行されて、請求項 10 記載の暗号化方法を実行する命令を格納する電子ストレージ媒体。

【請求項 29】

請求項 10 記載の暗号化方法によって暗号化されたテレビジョン信号を搬送する電子伝送媒体。

20

【請求項 30】

コンテンツを暗号化する暗号化方法において、

第 1 の暗号化法に基づいてコンテンツを暗号化し、第 1 の暗号化された部分を生成するステップと、

上記第 1 の暗号化された部分を暗号化されていないコンテンツ部分に結合し、部分的に暗号化されたコンテンツを生成するステップを有する暗号化方法。

【請求項 31】

上記部分的に暗号化されたコンテンツは、テレビジョン信号を含むことを特徴とする請求項 30 記載の暗号化方法。

【請求項 32】

上記部分的に暗号化されたテレビジョン信号をケーブルシステム、地上波放送システム、衛星システム、パッケージ媒体のいずれかを介して、配信するステップを更に有する請求項 31 記載の暗号化方法。

30

【請求項 33】

オーディオビジュアルコンテンツ配信システム内において、複数のアクセス制御システムを管理する管理方法において、

コンテンツの 100% 未満を複製する選択アルゴリズムに基づいて、上記複数のアクセス制御システムに対して複製するコンテンツの部分を識別するステップと、

上記識別されたコンテンツの部分を複製するステップとを有する管理方法。

【請求項 34】

上記識別され、複製された部分を第 1 の暗号化アルゴリズムを用いて暗号化するステップを更に有する請求項 33 記載の管理方法。

40

【請求項 35】

上記識別された部分を 2 回複製し、第 2 の複製された部分を生成するステップと、

第 2 の暗号化アルゴリズムを用いて、上記第 2 の複製された部分を暗号化するステップとを更に有する請求項 34 記載の管理方法。

【請求項 36】

上記識別された部分を、上記複製され、暗号化された部分及び第 2 の複製され、暗号化された部分に結合し、デュアル部分暗号化されたコンテンツを生成するステップを更に有する請求項 35 記載の管理方法。

50

【請求項 37】

ケーブルシステム、地上波放送システム、衛星システム、パッケージ媒体のいずれかを介して、上記デュアル部分暗号化されたテレビジョン信号を配信するステップを更に有する請求項 36 記載の管理方法。

【請求項 38】

上記識別されたコンテンツ、上記複製され、暗号化された部分及び上記第 2 の複製され、暗号化された部分を含むパケットにそれぞれ個別のパケット識別子を割り当てるステップを更に有する請求項 36 記載の管理方法。

【請求項 39】

上記コンテンツは、テレビジョンコンテンツを含むことを特徴とする請求項 33 記載の管理方法。

10

【請求項 40】

パケット化されたデジタルテレビジョン信号を符号化する符号化方法において、
第 1 の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含むパケットの一部を暗号化するステップと、
第 2 の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含むパケットの一部を暗号化するステップと、
デジタルテレビジョン信号を含むパケットの一部を暗号化せずにそのまま残すステップと、

上記暗号化されていないパケットに第 1 のパケット識別子を割り当てるステップと

20

上記第 1 の暗号化アルゴリズムに基づいて暗号化されたパケットに第 1 のパケット識別子を割り当てるステップと、

上記第 2 の暗号化アルゴリズムに基づいて暗号化されたパケットに第 2 のパケット識別子を割り当てるステップとを有する符号化方法。

【請求項 41】

上記デジタルテレビジョン信号を上記第 1 及び第 2 のパケット識別子にリンクする情報を生成するステップを更に有する請求項 40 記載の符号化方法。

【請求項 42】

上記デジタルテレビジョン信号を上記第 1 及び第 2 のパケット識別子にリンクする情報を番組特定情報 (PSI) として送信するステップを更に有する請求項 41 記載の符号化方法。

30

【請求項 43】

ケーブルシステム、地上波放送システム、衛星システムのいずれかを介して、上記暗号化されていないパケットを上記第 1 及び第 2 の暗号化アルゴリズムに基づいて暗号化されたパケットとともに送信するステップを更に有する請求項 40 記載の符号化方法。

【請求項 44】

衛星信号デスクランブラからクリアなパケットのストリームを受信する入力手段と、デュアル暗号化するパケットのグループを選択するとともに、クリアなパケットの組を残す選択手段と、

上記選択されたパケットを複製し、第 1 及び第 2 の複製されたパケットの組を生成する複製手段と、

40

第 1 のパケット識別子を第 1 の複製されたパケットの組に割り当て、第 2 のパケット識別子を第 2 の複製されたパケットの組に割り当てる割り当て手段と、

上記第 1 の複製されたパケットの組と、上記第 2 の複製されたパケットの組と、上記クリアなパケットの組とを多重化してパケットの出力ストリームを生成する多重化手段とを備えるパケット選択及び複製装置。

【請求項 45】

第 1 の暗号化アルゴリズムに基づいて上記第 1 の複製されたパケットの組及び上記クリアなパケットの組を暗号化する第 1 の暗号化器を更に備える請求項 44 記載のパケット選択及び複製装置。

50

【請求項 4 6】

第 1 の暗号化アルゴリズムに基づいて、上記第 1 のパケット識別子を有するパケットを暗号化する第 1 の暗号化器を更に備える請求項 4 4 記載のパケット選択及び複製装置。

【請求項 4 7】

第 2 の暗号化アルゴリズムに基づいて、上記第 2 の複製されたパケットの組を暗号化する第 2 の暗号化器を更に備える請求項 4 4 記載のパケット選択及び複製装置。

【請求項 4 8】

上記クリアなパケットのストリームは、システム情報を有するパケットを更に含み、上記第 2 の複製されたパケットの組を暗号化するために用いた暗号化法を特定するように上記システム情報を変更する変更手段を更に備える請求項 4 7 記載のパケット選択及び複製装置。

10

【請求項 4 9】

第 2 の暗号化アルゴリズムに基づいて、第 2 のパケット識別子を有するパケットを暗号化する第 2 の暗号化器を更に備える請求項 4 4 記載のパケット選択及び複製装置。

【請求項 5 0】

上記第 1 の複製されたパケットの組とクリアなパケットの組とが同じパケット識別子に割り当てられるようにパケット識別子を再マッピングするパケット再マッピング手段を更に備える請求項 4 4 記載のパケット選択及び複製装置。

【請求項 5 1】

デュアル暗号化のためのパケットのグループを選択する上記選択手段は、エレメンタリストリームパケットヘッダを含むパケットを選択するパケットと判定することを特徴とする請求項 4 4 記載のパケット選択及び複製装置。

20

【請求項 5 2】

デュアル暗号化のためのパケットのグループを選択する上記選択手段は、時間に依存するアルゴリズムに基づいて、パケットを選択することを特徴とする請求項 4 4 記載のパケット選択及び複製装置。

【請求項 5 3】

デュアル暗号化のためのパケットのグループを選択する上記選択手段は、オーディオ情報を含むパケットを選択するパケットと判定することを特徴とする請求項 4 4 記載のパケット選択及び複製装置。

30

【請求項 5 4】

デュアル暗号化のためのパケットのグループを選択する上記選択手段は、ビデオ情報を含むパケットを選択するパケットと判定することを特徴とする請求項 4 4 記載のパケット選択及び複製装置。

【請求項 5 5】

デュアル暗号化のためのパケットのグループを選択する上記選択手段は、システム情報を含むパケットを選択するパケットと判定することを特徴とする請求項 4 4 記載のパケット選択及び複製装置。

【請求項 5 6】

第 1 のパケット識別子を有するクリアなパケットと、第 2 のパケット識別子を有する暗号化されたパケットと、第 3 のパケット識別子を有する暗号化されたパケットとを含む変調されたパケットのストリームを復調する復調器と、

40

上記第 1 のパケット識別子を有するクリアなパケットと、上記第 2 のパケット識別子を有する暗号化されたパケットとが同じパケット識別子を有するように上記パケット識別子を変更する再マッピング器とを備えるパケット識別子再マッピング装置。

【請求項 5 7】

上記第 3 のパケット識別子を有するパケットは、クリアなパケットを含み、上記第 2 のパケット識別子を有するパケットを暗号化するアルゴリズムとは異なるアルゴリズムで、該第 3 のパケット識別子を有するパケットを暗号化する暗号化器を更に備えることを特徴とする請求項 5 6 記載のパケット識別子再マッピング装置。

50

【請求項 5 8】

第 3 のパケット識別子を有するパケットは、暗号化されたパケットを含み、
該第 3 のパケット識別子を有するパケットは、上記第 2 のパケット識別子を有するパケットを暗号化するアルゴリズムとは異なるアルゴリズムで暗号化されていることを特徴とする請求項 5 6 記載のパケット識別子再マッピング装置。

【請求項 5 9】

上記変調されたパケットのストリームは、直交振幅変調されており、上記復調器は、直交振幅復調器であることを特徴とする 5 6 記載のパケット識別子再マッピング装置。

【請求項 6 0】

上記再マッピングされたパケットを第 3 のパケット識別子を有するパケットに結合して出力データストリームを生成するマルチプレクサを更に備える請求項 5 6 記載のパケット識別子再マッピング装置。

10

【請求項 6 1】

上記出力データストリームを変調する直交振幅変調器を更に備える請求項 6 0 記載のパケット識別子再マッピング装置。

【請求項 6 2】

上記変調されたパケットのストリームは、システム情報を有するパケットを含み、
上記第 3 のパケット識別子を有するパケットを暗号化した暗号化法を特定するように上記システム情報を変更する変更手段を更に備えることを特徴とする請求項 5 6 記載のパケット識別子再マッピング装置。

20

【請求項 6 3】

テレビジョンプロバイダヘッドエンドにおいて実行される処理方法において、
スクランプリングされたテレビジョンコンテンツをパケットのストリームの形式で受信するステップと、

上記スクランプリングされたテレビジョンコンテンツをデスクランブルして、クリアなパケットのストリームを生成するステップと、

デュアル暗号化のためのパケットを選択するステップと、

上記パケットを複製し、第 1 及び第 2 のパケットを生成するステップと、

上記第 1 及び第 2 パケットに、第 1 及び第 2 のパケット識別子を再マッピングするステップと、

30

上記第 1 のパケットを第 1 の暗号化アルゴリズムに基づいて暗号化し、第 1 の暗号化されたパケットを生成するステップと、

上記第 2 のパケットを第 2 の暗号化アルゴリズムに基づいて暗号化し、第 2 の暗号化されたパケットを生成するステップと、

上記第 1 のパケット識別子に、クリアなパケットを再マッピングするステップとを有する処理方法。

【請求項 6 4】

クリアなパケットと、上記第 1 のパケット及び第 2 のパケットとを結合することによって、部分的に暗号化されたパケットのストリームを組み立てるステップを更に有する請求項 6 3 記載の処理方法。

40

【請求項 6 5】

上記第 1 及び第 2 パケットは、上記部分的に暗号化されたパケットのストリーム内に互いに隣接するように挿入されることを特徴とする請求項 6 3 記載の処理方法。

【請求項 6 6】

上記パケットは、該パケットのコンテンツに基づいて、デュアル暗号化のために選択されることを特徴とする請求項 6 3 記載の処理方法。

【請求項 6 7】

上記パケットは、上記クリアなパケットのストリームのサンプリングのためのタイミングシーケンスに基づいて、デュアル暗号化のために選択されることを特徴とする請求項 6 3 記載の処理方法。

50

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号化システムに関し、より詳しくは、デジタルテレビジョン信号の部分的な暗号化及び復号を行うシステム、方法及び装置に関する。

【0002】

[関連出願]

本出願は、2001年6月6日に出願されたカンデロア他の米国仮出願番号第60/296,673号「あるコンテンツのビデオをクリアに、及び他のコンテンツのビデオ及びオーディオのデュアルキャリアジを送信することによって、複数のCAプロバイダがコンテンツ配信システムにおいて相互運用を行うことができる方法(Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Sending Video in the Clear for Some Content, and Dual Carriage of Audio and Dual Carriage of Video and Audio for Other Content)」、2001年7月10日に出願されたアンガー他の米国仮出願番号第60/304,241号「デュアルキャリアジのプログラムコンテンツの自由に選択可能な暗号(Independent Selective Encryptions of Program Content for Dual Carriage)」、2001年7月10日に出願されたカンデロア他の米国仮出願番号第60/304,131号「タイムスライス方式においてコンテンツに部分的にスクランブルを掛けることによって、複数のCAプロバイダが相互運用を行うことができる方法(Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Partial Scrambling Content on a Time Slice Basis)」及び2001年10月26日に出願されたカンデロア他の米国仮出願代理人整理番号SNY-R4646P「テレビジョン暗号化システム(Television Encryption System)」に関連し、これら関連出願は、参照により本願に援用される。

【0003】

本出願は、アンガー他の米国特許出願代理人整理番号SNY-R4646.01「重要なパケットの部分的な暗号化(Critical packet Partial Encryption)」、カンデロア他の米国特許出願代理人整理番号SNY-R4646.02「時間分割の部分的な暗号化(Time Division Partial Encryption)」、アンガー他の米国特許出願代理人整理番号SNY1-R4646.03「エレメンタリストリーム部分暗号化(Elementary Stream Partial Encryption)」、及びアンガー他の米国特許出願代理人整理番号SNY-R4646.05「部分的に暗号化された情報の復号及び解読(Decoding and Decrypting of Partially Encrypted Information)」と同時に提出されている。これらの同時に出願された米国出願は、参照により本願に援用される。

【0004】

[著作権表示]

この明細書の開示内容の一部は、著作権保護の対象となる資料を含んでいる。著作権者は、この明細書が特許商標庁への特許出願又は記録であると認められるファックスコピー又は特許開示に対しては異議を唱えないが、それ以外のあらゆる全ての著作権を保有する。

【背景技術】

【0005】

テレビジョンシステムは、視聴者に娯楽番組及び教育番組を配信するために用いられる。ソースマテリアル(オーディオデータ、ビデオデータ等)は、混合信号(combined signal)に多重化され、この混合信号は搬送波を変調するために用いられる。この搬送波は、一般に、チャンネルとして知られている(典型的なチャンネルでは、1つのアナログ番組、1つ又は2つの高精細度(HD)デジタル番組、又は複数の(例えば9つの)標準解像度のデジタル番組を送ることができる)。地上波システムにおいて、これらのチャンネルは、行政割当の周波数(government assigned frequencies)に対応し、電波によって放送される。番組は、受信機に配信され、受信機はチューナを備え、チューナは、電波か

10

20

30

40

50

ら信号を検波して、復調器に供給し、復調器は、映像をディスプレイに、音声をスピーカから出力する。ケーブルシステムにおいては、変調チャンネルは、ケーブルを介して送られる。また、視聴可能な番組及び関連した選局情報を示す番組ガイドを、チャンネルの帯域内又は帯域外で提供することもできる。ケーブルシステムではチャンネルの数は、限られており、すなわち機器及びケーブルの帯域幅によって制限される。ケーブルの敷設 (CABLE distribution systems) には、巨額の設備投資がかかり、その改良にも費用がかかる。

【 0 0 0 6 】

テレビジョンコンテンツの多くは、その製作者にとって貴重なものであり、したがって、著作権者は、アクセスを制御し、コピーを制限することを望んでいる。典型的な著作権保護の材料 (protected material) の例としては、長編映画 (feature film)、スポーツ競技の番組、成人番組がある。限定受信 (conditional access: 以下 C A という。) 方式は、ケーブルシステム等のコンテンツ配信システムにおける番組の視聴 (availability) を制御するために用いられる。C A 方式は、ケーブルシステムのヘッドエンドに組み込まれ、有料コンテンツ (premium content) を暗号化する部分と、ユーザの家庭に設置されたセットトップボックス (set-top box: 以下 S T B という。) に内蔵され、復号を行う部分との組合せ (matched set) として提供される。ケーブルテレビ業界では、N D S 社 (米国カリフォルニア州ニューポートビーチ)、モトローラ社 (米国イリノイ州シウンバーグ)、サイエンティフィックアトランタ社 (米国ジョージア州アトランタ) によって提供されている C A 方式を含む幾つかの C A 方式が使用されている。C A 方式における暗号化部と復号部を整合させなければならないという状況により、「旧型 ("legacy")」の S T B の製造業者は、この S T B を供給し続けなければならない。限定受信の様々な技術は、互換性がない (且つ、多くの場合、独占 (proprietary) されている) ので、新規に参入する供給業者は、旧式の C A 方式のライセンスを受けることを余儀なくされる。したがって、C A 方式技術の保有者は、多くの場合、協力又は適正な実施料を請求する気がなく、ケーブルテレビの運用業者は、他のセットトップボックス製造業者からより新しい技術又は競合する技術を取得することができない。このように技術的互換性がないために、異なる C A 方式を採用しているケーブルテレビ会社が合併する際には、特に問題がある。サービス提供業者は、数多くの理由から、S T B 供給元が複数あることを希望する。

【 0 0 0 7 】

ケーブルテレビ運用業者は、一旦、あるコンテンツ暗号化方式 (encryption scheme) を採用すると、下位互換性のある復号装置 (例えばセットトップボックス) を導入することなく、そのコンテンツ暗号化方式を変更又は更新することは困難になる。S T B の製造業者は、複数の復号機能を提供する技術があっても、新しいセットトップボックスに複数の暗号化方式に対応するようなマルチモード機能を付けると、この新しいセットトップボックスにはかなりの原価がかかってしまう。

【 0 0 0 8 】

旧型の S T B の製造業者による支配を避けるための現在知られている唯一の選択肢は、(大規模な交換を除いて) 「フルデュアルキャリッジ (full dual carriage)」を用いることである。フルデュアルキャリッジとは、それぞれの暗号化された番組に対して、用いられている C A 暗号化の種類毎に、二重に伝送することを意味する。フルデュアルキャリッジを提供するためには、ヘッドエンドを、各 C A 方式を同時に提供するように増強しなければならない。如何なる変更があった場合でも、旧型の S T B は、影響を受けず、その機能を実行し続けなければならない。しかしながら、フルデュアルキャリッジでは、多くの場合、帯域が重なることを避けるためには視聴可能な番組の数を減らさなければならず、受け入れ難い料金となっている。通常、有料チャンネルの数が少なくなると、視聴者の視聴可能な選択肢も限定され、ケーブルテレビ運用業者が提供できる価値も制限される。

【 0 0 0 9 】

図 1 は、従来のケーブルシステムの構成を示すブロックである。このケーブルシステム

では、ケーブルテレビ運用業者は、ケーブルシステムヘッドエンド 2 2 において方式 A に準拠した C A 暗号化装置 1 8 を用い、製造業者 A (方式 A) の C A 技術によってオーディオ/ビデオ (A/V) コンテンツ 1 4 を処理する。暗号化された A/V コンテンツは、システム情報 (system information: 以下 S I という。) 2 6 及び番組特定情報 (program specific information: 以下 P S I という。) 2 7 が多重化され、ケーブルシステム 3 2 を介してユーザの S T B 3 6 に伝送される。S T B 3 6 には、暗号化された A/V コンテンツを復号する C A 方式 A (製造業者 A) の C A 復号装置が組み込まれている。復号された A/V コンテンツは、テレビジョン受信機 4 4 に供給され、ユーザによって視聴される。

【 0 0 1 0 】

図 1 に示すようなケーブルシステムにおいて、デジタル番組ストリームはパケットに分割されて伝送される。番組の各コンポーネント (ビデオデータ、オーディオデータ、補助データ等) のパケットには、パケット識別子 (packet identifier: 以下 P I D という。) が付加される。チャンネル内で送られる全ての番組の各コンポーネントに対するこれらのパケットストリームは、1つの複合ストリームに結合される。複合ストリームは、復号鍵及び他のオーバーヘッド情報を有する追加的なパケットも含んでいる。追加的なパケットがない場合、未使用の帯域は空パケットによって埋められる。帯域配分は、通常、利用可能なチャンネル帯域幅の約 9 5 % を使用するように調整されている。

【 0 0 1 1 】

オーバーヘッド情報は、通常、視聴可能な番組と、その関連するチャンネル及びコンポーネントの位置を特定する方法を示すガイドデータを含んでいる。このガイドデータは、システム情報、すなわち S I としても知られている。S I は、S T B に帯域内で (チャンネル内の暗号化データの一部として) 又は帯域外で (この目的専用に設けられた特別のチャンネルを用いて) 配信することができる。電子的に配信される S I は、従来の種類の、すなわち新聞及び雑誌に記載された番組表を部分的に複製したものでよい。

【 0 0 1 2 】

視聴者が満足の得られるテレビジョンの視聴をするためには、一般的に、暗号化されていない状態で (clear) オーディオコンテンツ及びビデオコンテンツの両方にアクセスできることが望ましい。幾つかのアナログケーブルシステムでは、料金を払っていない未許可の視聴者が番組を受信できないように、様々なフィルタリング技術を用いてビデオコンテンツを見えなくしている。このようなアナログケーブルシステムにおいては、アナログオーディオコンテンツは、鮮明 (clear) に送られることもある。C バンド衛星通信に用いられるモトローラ社のビデオサイファ 2 プラス (VideoCipher 2 Plus、商標) 方式では、強力なデジタルオーディオ暗号化と、アナログビデオデータの比較的弱い (同期反転を用いた) 保護との組合せが用いられている。航空会社の機内映画システムでは、料金を払ってヘッドホンを借りた乗客のみが、オーディオとビデオを完全に視聴できるという方法を用いている。

【 0 0 1 3 】

本発明を特定の具体例を用いて説明してきたが、当業者は、上述の説明から多くの代替例、修正例、変更例、変形例を想到することができる。これらの代替例、修正例、変更例、変形例は、本発明の範囲内にある。

【 図面の簡単な説明 】

【 0 0 1 4 】

【 図 1 】 従来の限定受信ケーブルシステムの構成を示すブロック図である。

【 図 2 】 本発明の実施例として示す、デュアル暗号化オーディオデータをクリアなビデオデータとともに伝送するシステムの構成を示すブロック図である。

【 図 3 】 本発明の実施例として示す、番組の一部がタイムスライスメカニズムに基づいて、デュアル暗号化されるシステムの構成を示すブロック図である。

【 図 4 】 本発明の実施例として示す、デュアル暗号化処理のフローチャートである。

【 図 5 】 本発明の実施例として示す、暗号化処理のフローチャートである。

10

20

30

40

50

【図 6】本発明の実施例として示す、番組の一部がパケット毎にデュアル暗号化されるシステムの構成を示すブロック図である。

【図 7】本発明の実施例として示す、デュアル暗号化処理のフローチャートである。

【図 8】本発明の実施例として示す、暗号化処理のフローチャートである。

【図 9】本発明の実施例として示す、システム情報が暗号化され、番組がクリアな形式で伝送されるシステムの構成を示すブロック図である。

【図 10】本発明の様々な実施例に対応する包括的なシステムの構成を示すブロック図である。

【図 11】本発明の実施例として示す、ケーブルシステムヘッドエンドの第 1 の実現例を示すブロック図である。

10

【図 12】本発明の実施例として示す、ケーブルシステムヘッドエンドの第 2 の実現例を示すブロック図である。

【図 13】本発明の実施例として示す、ケーブルシステムヘッドエンドにおける暗号化処理のフローチャートである。

【図 14】本発明の実施例として示す、セットトップボックスによって実現されたデコードシステムの第 1 の実現例を示すブロック図である。

【図 15】本発明の実施例として示す、ケーブルシステム S T B によって実現されたデコードシステムの第 2 の実現例を示すブロック図である。

【図 16】本発明の実施例として示す、ケーブルシステム S T B によって実現されたデコードシステムの第 3 の実現例を示すブロック図である。

20

【図 17】本発明の実施例において、セットトップボックス P I D 再マッピング器により実行される P I D 再マッピング処理を説明する図である。

【図 18】本発明に基づくセットトップボックスにおいて用いられるデコーダチップの具体的構成例を示す図である。

【発明を実施するための形態】

【0015】

本発明は、数多くの異なる構成の実施例があるが、図面を参照して詳細に説明する特定の実施例は、開示内容が本発明の趣旨の一例とみなされるものであり、本発明をその特定の実施例に限定するものではない。後述する実施例において、類似の参照番号は、複数の図面における同じ、類似、又は対応する部分には、同じ参照番号を付している。用語「スクランブル (scramble)」、「暗号化 (encrypt)」及びその活用形は、ここでは同義で用いられている。また、用語「テレビジョン番組 (television program)」及び類似の用語は、日常会話に使用する意味とともに、テレビジョン受信機又は同様のモニタ装置に表示することができる A / V コンテンツのいずれかのセグメントの意味にもなる。

30

【0016】

概要

現在のデジタルケーブルネットワークは、多くの場合、デジタルオーディオデータ及びビデオデータを完全に暗号化する C A 方式を用いて、適切に申込みをした加入者以外は番組を視聴することができないようにしている。この暗号化は、ハッカー及び料金を払っていない未加入者が番組を受信することができないようにすることを目的としている。しかしながら、ケーブルテレビ運用業者は、加入者に複数のセットトップボックス製造業者のいずれの製品でも提供することができることを望んでいるため、それぞれの S T B 製造業者の C A 方式に対応した複数の暗号化技術を用いて、1つの番組を複数暗号化したコピーを送信しなければならない。

40

【0017】

番組の複数のコピーを伝送する（「フルデュアルキャリッジ」という。）必要があると、視聴者に更なる番組のコンテンツを提供することができる貴重な帯域幅も使い果たしてしまう。本発明の一実施例では、この問題に対応するために、複数のキャリッジと等価なもの (equivalent) を伝送するために必要な帯域幅を最小限に抑えるようにしてる。この結果、帯域全体を使用することなく、フルデュアルキャリッジと同等の効果を得ることが

50

できるので、この方式を「仮想デュアルキャリッジ (Virtual Dual Carriage)」と呼ぶ。本発明の幾つかの実施例では、部分的なスクランブルを効果的に実現する。どの部分を暗号化するかを選択する基準によって、様々な実施例がある。選択する部分によって、新たに必要とされる帯域幅と、暗号化の効果とが変わる。本発明の実施例に矛盾しない方法で、1つの暗号化処理又は複数の暗号化処理の組合せを用いることが好ましい。

【0018】

ここに開示する部分デュアル暗号化 (partial dual encryption) では、複製された各コンポーネントに対して、追加的な (すなわち第2の) パケット識別子 (PID) を用いる。これらの第2のPIDは、他の暗号化方法によって暗号化されたコンテンツのコピーを伝送するパケットのタグとして用いられる。番組特定情報 (PSI) は、挿入された第2のPIDが旧型のSTBでは無視され、新型のSTBでは容易に抽出することができるように、これら新しい第2のPIDの存在に関する情報を伝送するように拡張されている。

10

【0019】

部分デュアル暗号化の実施例には、所定のPIDを有するパケットのみを複製することにも含まれる。暗号化するパケットの選択方法は、後で詳述する。元の (すなわち旧) PIDは、依然として、暗号化されずに (in the clear) 送信されるパケットだけではなく、旧暗号化方式で暗号化されたパケットにもタグとして付される。新PIDは、第2の暗号化方法によって暗号化されたパケットのタグとして用いられる。第2のPIDが付けられたパケットは、第1のPIDが付された暗号化パケットを隠す (shadow)。暗号化されたペアを構成する (making up) パケットは、いずれの順番で伝送されてもよいが、PIDストリームの暗号化されていない部分のシーケンスを保つことが好ましい。以下の説明から明らかのように、第1と第2のPIDを用いることにより、セットトップボックスに内蔵された復号器は、そのセットトップボックス自体の復号方法を用いて、どのパケットを復号するかを容易に判定することができる。PIDの処理方法については後で詳細に説明する。

20

【0020】

ここに説明する暗号化技術は、(1つの分類方法として) 大きく3つに、すなわち主要部 (すなわちオーディオデータ) のみを暗号化する技術と、SIのみを暗号化する技術と、選択されたパケットのみを暗号化する技術とに分類することができる。一般的に、ここに説明する実施例に用いられる各暗号化技術は、A/V信号の一部又は関連する情報を暗号化し、A/V信号の残りの部分をクリア (clear) にして帯域幅を節約する。帯域幅の節約が可能である理由は、同一のクリアな部分を、全ての種類のセットトップボックスに送信することができるためである。情報の暗号化する部分を選択するには、様々な方法が用いられる。これにより、本発明の様々な実施例では、1つの特定のスクランブル方式でコンテンツ全体を暗号化する従来の「強引な (brute-force)」、すなわち2つ以上のスクランブル方式が望まれる場合において帯域を冗長に浪費する技術を用いないで済む。また、ここに説明する各部分デュアル暗号化方式は、本発明の実施例から逸脱することなく、1つの部分暗号化方式として用いることができる。

30

【0021】

本発明の様々な実施例では、複数の処理を単独又は組み合わせて用いて、コンテンツの実質的な部分 (substantial portions) をクリアな形式で (暗号化せずに) に送り、一方、コンテンツを正しく再生するのに必要とされるデータ量の少ない情報のみを暗号化する。したがって、所望の各番組ストリームの全体をコピーするのに対し、特定のスクランブル方式で独自に暗号化され、伝送される情報量は、コンテンツのほんの一部である。この明細書における具体的なシステムでは、暗号化方式Aは旧式であるとみなしている。上述した幾つかの暗号化技術を、以下に詳細に説明する。

40

【0022】

本発明の様々な実施例において用いられる各CA方式は、独立して動作することができる。各CA方式は、他の方式と直交している。各CA方式は、それ自体の特徴 (patents

50

)を暗号化するので、ヘッドエンドにおける鍵の共用は不要である。各CA方式において、異なる暗号鍵方式(different key epochs)を用いてもよい。例えば、モトローラ社所有の暗号化方式によって暗号化されたパケットは、組込みセキュリティASICによって発生された高速変更暗号鍵(fast changing encryption keys)を用いることができ、一方、NDS社のスマートカードベースの方式で暗号化されたパケットは、それより僅かに遅い変更暗号鍵を用いることができる。この実施例のシステムは、サイエンティフィックアトランタ社及びモトローラ社の旧式の暗号化方式に対しても同等にうまく動作する。

【0023】

暗号化エレメンタリストリーム(ENCRYPTED ELEMENTARY STREAM)

図2に示すシステム100は、複数のキャリアッジを提供するために帯域幅を追加する必要性を減らすシステムの一実施例である。この実施例において、システム100は、音声を聞かないでテレビジョン番組を見ることは普通好まれないという事実を利用している。例外(例えば成人番組、ある種のスポーツ競技番組等)はあるが、一般的な視聴者は、日常、音声を聞くことができないでテレビジョン番組を見ることは受け入れ難い。したがって、ヘッドエンド122において、ビデオデータ104はクリアに(暗号化しないで)ケーブルネットワークを介して放送するが、クリアなオーディオデータ106は複数のCA装置に供給した後、放送する。具体的なシステム100においては、クリアなオーディオデータ106は、暗号化方式Aを用いてオーディオデータを暗号化する暗号化装置118に供給される(暗号化方式Aは、この明細書中では旧式の暗号化方式とする)。同時に、クリアなオーディオデータ106は、暗号化方式Bを用いてオーディオデータを暗号化する暗号化装置124に供給される。そして、クリアなビデオデータには、暗号化装置118、124からの暗号化されたオーディオデータ(オーディオA、オーディオB)と、システム情報128と、番組特定情報129とが多重化される。

【0024】

ビデオデータ、システム情報、番組特定情報、オーディオA及びオーディオBの全ては、ケーブルシステム32を介して配信された後、セットトップボックス(STB)36、136で受信される。旧型のSTB36において、ビデオデータはテレビジョン受信機44で表示され、暗号化オーディオデータは、CA方式A40によって復号され、テレビジョン受信機44で再生される。同様に、新型のSTB136において、ビデオデータはテレビジョン受信機144で表示されるとともに、暗号化オーディオデータは、CA方式B140によって復号され、テレビジョン受信機144で再生される。

【0025】

オーディオデータは、完全なA/Vプログラムに比して(又はビデオデータのみ部分と比べても)、必要とされる帯域幅は相対的に少ない。ステレオのオーディオデータを384kb/sで送信する場合、現在の最大ビットレートは、3.8Mb/sのテレビジョン番組の約10%である。したがって、256QAM(直交振幅変調)で送られる10チャンネルのシステムにおいて、暗号化オーディオデータのみデュアルキャリアッジ(ビデオデータは暗号化しないで伝送される)では、約1チャンネル分の帯域幅の損失(loss)しか発生しない。したがって、約9チャンネルを送信することができる。このことは、全てのチャンネルをデュアル暗号化する必要があると、送信可能なチャンネル数が10から5に減少する場合に比して、大幅な改善である。なお、例えばスポーツ競技の番組、ペイパービューの番組、成人番組等において、必要がある場合には、オーディオデータとビデオデータの両方を、今まで通りデュアル暗号化することもできる。

【0026】

旧型のセットトップボックスと新型のセットトップボックスの両方とも、クリアなビデオデータを通常の方法で受信するとともに、暗号化A/Vコンテンツを完全に復号するのに用いられる方法と同じ方法で、オーディオデータを復号するように機能することができる。ユーザが、上述した方法で暗号化された番組を視聴する申込みをしていない場合、ユーザは、良くて、音声を聞かないで映像を見ることのできるだけである。ビデオデータのセキュリティを上げるためには、ここで本発明の(後述する)他の実施例を用いること

10

20

30

40

50

もできる。(例えば、S Iにスクランブルを掛けて、未許可のセットトップボックスが番組のビデオデータ部分を選局することが難しくなるようにしてもよい。)未許可であって、ハッカーによって改造されていないセットトップボックスは、暗号化オーディオデータを受信すると、映像を消して(blank)しまう。

【0027】

許可されたセットトップボックスは、アクセス基準(access criteria)及びデスクランブル鍵を受け取るために用いられる資格制御メッセージ(Entitlement Control Message:以下ECMという。)を受信する。このセットトップボックスは、デスクランブル鍵をオーディオデータだけでなく、ビデオデータに対しても適用する。ビデオデータは、スクランブルが掛かっていないので、セットトップボックスのデスクランブラをそのまま通過する。セットトップボックスは、ビデオデータがクリアあるかを考慮しない。未改造(un-modified)且つ未加入(un-subscribed)のセットトップボックスは、クリアなビデオデータとスクランブルが掛かったオーディオデータに対して、未許可(un-authorized)のセットトップボックスとして動作する。オーディオデータだけではなく、ビデオデータにも実際にスクランブルが掛かっている場合には、映像は表示されない。そして、画面上に、視聴者が番組を視聴するためには申込みが必要であることを示すオンスクリーンディスプレイが現れるようにしてもよい。これにより、視聴者が偶然、コンテンツを聞くことと、見ることの両方を完全に防止することができる。

10

【0028】

本発明の一実施例において、暗号化オーディオデータは、デジタルパケットとしてA/Vチャンネルを介して配信される。2つ(又は2つ以上)のオーディオストリームは、システム100のセットトップボックスで採用されている2つ(又は2つ以上)の暗号化方式に基づいてそれぞれ暗号化されて、伝送される。2つ(又は2つ以上)のSTBにおいて、それぞれのオーディオストリームを適切に復号及びデコードするために、システム100のヘッドエンド122から、伝送サービス識別子(Service Identifier)を用いてオーディオデータが位置するチャンネルを検出するためのSI(システム情報)データが送信される。この処理は、CA方式A40のオーディオデータに対して第1のパケット識別子(PID)を割り当て、CA方式B140のオーディオデータに対して第2のパケット識別子(PID)を割り当てることにより実現される。限定されるものではないが、一具体例として、以下の番組特定情報(PSI)を、NDS社とモトローラ社の限定受信技術をそれぞれ用いた2つのCA方式におけるオーディオデータの位置を指定するために送ってもよい。この番組特定情報を後述する部分暗号化の他の実施例に適用できることは、当業者に明らかである。

20

30

【0029】

SIは、旧型のセットトップボックスと非旧型のセットトップボックスの両方に別々に送信することができる。また、SIは、旧型のセットトップボックスと非旧型のセットトップボックスが基本的に混信することなく動作するように、送信することができる。旧型のセットトップボックスに配信されるSI内の仮想チャンネルテーブル(virtual channel table:VCT)は、所望の番組、例えばプログラム番号1として参照されるHBOはサービスIDが「1」であり、VCTアクセス制御ビットが設定されていることを示している。旧型のセットトップボックスに配信されるネットワーク情報テーブル(network information table:NIT)は、サービスID「1」が周波数1234であることを示している。また、非旧型のセットトップボックスに配信されるSI内のVCTは、所望の番組、例えばプログラム番号1001で参照されるHBOはサービスIDが「1001」であり、VCTアクセス制御ビットが設定されていることを示している。非旧型のセットトップボックスに配信されるNITは、サービスID「1001」が周波数1234であることを示している。以下に例示的に示す放送番組関連テーブル(program association table:PAT)のPSIデータは、旧型と非旧型のセットトップボックスの両方に(MPEGデータ構造フォーマットで)送信される。

40

【0030】

50

【表 1】

PID=0x0000 で伝送される PAT	
PAT 0x0000	
- トランスポートストリーム ID	
- PAT バージョン	
- 番組番号 1	
- PMT 0x0010	10
- 番組番号 2	
- PMT 0x0020	
- 番組番号 3	
- PMT 0x0030	
- 番組番号 4	
- PMT 0x0040	
- 番組番号 5	
- PMT 0x0050	
- 番組番号 6	
- PMT 0x0060	
- 番組番号 7	20
- PMT 0x0070	
- 番組番号 8	
- PMT 0x0080	
- 番組番号 9	
- PMT 0x0090	
- 番組番号 1 0 0 1	
- PMT 0x1010	
- 番組番号 1 0 0 2	
- PMT 0x1020	
- 番組番号 1 0 0 3	30
- PMT 0x1030	
- 番組番号 1 0 0 4	
- PMT 0x1040	
- 番組番号 1 0 0 5	
- PMT 0x1050	
- 番組番号 1 0 0 6	
- PMT 0x1060	
- 番組番号 1 0 0 7	
- PMT 0x1070	
- 番組番号 1 0 0 8	40
- PMT 0x1080	
- 番組番号 1 0 0 9	
- PMT 0x1090	

【 0 0 3 1 】

以下の具体的な放送番組マップテーブル (program map table: PMT) の P S I データは、旧型及び非旧型のセットトップボックスによって (M P E G データ構造フォーマットで) 選択的に受信される。

【 0 0 3 2 】

【 表 2 】

<p>PID=0x0010 で伝送される PMT</p> <p>PMT 0x0010</p> <ul style="list-style-type: none">- PMT 番組番号 1- PMT セクションバージョン 1 0- PCR PID 0x0011- エレメンタリストリーム<ul style="list-style-type: none">- ストリームタイプ (ビデオ 0x20 又は 0x80)- エレメンタリ PID (0x0011)- 記述子<ul style="list-style-type: none">- CA プロバイダ # 1 用の CA 記述子(ECM)- エレメンタリストリーム<ul style="list-style-type: none">- ストリームタイプ (オーディオ 0x81)- エレメンタリ PID (0x0012)- 記述子<ul style="list-style-type: none">- CA プロバイダ # 1 用の CA 記述子(ECM)	10 20
<p>PID=0x1010 で伝送される PMT</p> <p>PMT 0x1010</p> <ul style="list-style-type: none">- PMT 番組番号 1 0 1 0- PMT セクションバージョン 1 0- PCR PID 0x0011- エレメンタリストリーム<ul style="list-style-type: none">- ストリームタイプ (ビデオ 0x02 又は 0x80)- エレメンタリ PID (0x0011)- 記述子<ul style="list-style-type: none">- CA プロバイダ # 2 用の CA 記述子(ECM)- エレメンタリストリーム<ul style="list-style-type: none">- ストリームタイプ (オーディオ 0x81)- エレメンタリ PID (0x0013)- 記述子<ul style="list-style-type: none">- CA プロバイダ # 2 用の CA 記述子(ECM)	30 50

【 0 0 3 3 】

NDS社のCA方式に加えて、モトローラ社とサイエンティフィックアトランタ社のいずれかのCA方式を採用したシステムにおいて、番組の配信に適した一具体例では、上述の通信は、少し変更するだけで、モトローラ社とサイエンティフィックアトランタ社の両方のCA方式で配信されるPSIとは矛盾しない。放送番組関連テーブル(PAT)は、各番組の追加的な放送番組マップテーブル(PMT)を参照するように変更される。この実施例において、各番組は、PAT内にそれぞれ2つのプログラム番号を有する。上記表1において、プログラム番号1及びプログラム番号1001は、同じ番組であるが、それぞれ異なる音声PID及びCA記述子を参照している。システム100において、複数のPMTを生成するとともに、新たなPAT及びPMTの情報をデータストリームに多重化する変更は、ケーブルシステム32のヘッドエンド装置を適切に変更することによって、行うことができる。また、これらのメッセージを明細書に記載の他の部分暗号化方式により暗号化できることは、当業者に明らかである。この方法では、ヘッドエンド、又は旧型

及び非旧型のセットトップボックスに特別なハードウェア又はソフトウェアを必要とせず、この方法を用いて旧式と非旧式の暗号化方式で暗号化されたオーディオ信号を配信することができるという利点がある。

【0034】

この技術により、ユーザが料金を支払っていない有料番組の音声を聞こえないようにして視聴を阻止することができるが、ハッカーは、映像を選局することができる。これに対抗するために、本発明の他の暗号化技術において用いられる（後述するような）機構（mechanisms）を、必要に応じて同時に使用してもよい。一般的に、文字多重情報はビデオデータの一部として伝送されているので、ユーザは、クリアな映像とともに、読める音声情報を得ることができる。したがって、この技術は、ある用途には向いているが、全ての用途に対しては、単独では十分な保護を与えとは言えない。他の実施例において、ペイロードの一部として文字多重情報を含むビデオパケットに、更にスクランブルを掛けてもよい。

10

【0035】

他の実施例において、ビデオデータのみをデュアル暗号化して、暗号化ビデオデータの各セットに別々のPIDを割り当ててもよい。これにより、（ビデオデータはオーディオデータより重要であるので）通常番組に対してより堅固な暗号化を提供することができるが、全てのセットトップボックスで共用されるのはオーディオデータのみであるので、節約できる帯域幅の量は、フルデュアルキャリッジに比べて僅かに約10%である。なお、この方法を、例えば成人番組及びスポーツ競技番組等のある特定のコンテンツに用いて、そのコンテンツに対する帯域幅のオーバーヘッドを削減し、他の種類のコンテンツに対してはオーディオ暗号化方法を用いてもよい。ディレクTV（DirecTV、商標）サービスで用いられているデジタル衛星サービス（Digital Satellite Service：DSS）のトランスポート規格（transport standard）においてパケット識別子と同等なものとみなされるサービスチャンネル識別子（service channel identifier：SCID）を用いて、オーディオパケットの暗号化を識別することができる。

20

【0036】

タイムスライシング

本発明の他の実施例は、タイムスライシングに関し、システム200として図3に示す。この実施例においては、各番組の一部を時間依存ベースで暗号化して、ユーザが番組視聴の支払いをしていないときには、番組の視聴を中止させる。本発明のこの実施例は、ビデオデータを部分的に暗号化するとともにオーディオデータをクリアなものとする、ビデオデータをクリアなものとするるとともにオーディオデータを部分的に暗号化する、或いはビデオデータ及びオーディオデータを部分的に暗号化することによって実現することができる。タイムスライス、すなわち暗号化されている期間の全時間に対する割合は、使用される帯域幅とハッカーに対する安全性とのバランスが最適になるように、選択することができる。一般的に、ここに述べるどの実施例においても、コンテンツを100%未満で暗号化し、所望の部分暗号化データを生成している。以下の具体例において、ビデオデータ及びオーディオデータの部分暗号化について説明する。

30

【0037】

一例として、且つこれに限定されるものではないが、本発明の具体的な実施例に基づいて9つの番組をデュアル部分暗号化（dual partially encrypt）システムを説明する。これらの9チャンネルは、パケットの多重化されたストリームとして、ケーブルヘッドエンド222に供給され、9つの番組のうち特定の1つの番組に関連したパケットを識別するためのパケット識別子（PID）を用いてデジタル的にエンコードされる。この具体例において、これら9つの番組は、101～109の番号が付けられたビデオPIDと、201～209の番号が付けられたオーディオPIDとを有しているとする。この実施例に基づいた部分暗号化は、任意の時間においては1つの番組のパケットのみが暗号化されるように、9つの番組に対して時分割的に行われる。この方法は、コンテンツが分かっている（content-aware）必要はない。

40

50

【 0 0 3 8 】

下記表 3 を参照して、本発明の実施例であるタイムスライスデュアル暗号化を説明する。第 1 のビデオ P I D 1 0 1 及び第 1 のオーディオ P I D 2 0 1 を有する番組 1 について、第 1 の期間では P I D 1 0 1 及び P I D 2 0 1 を有するパケットを暗号化方式 A を用いて暗号化し、他の番組を表す他のパケットをクリアに送信する。この実施例において、第 2 の P I D もビデオパケット及びオーディオパケットに対して割り当てられている。番組 1 の第 2 の P I D は、ビデオパケットに対しては P I D 1 1 1 であり、オーディオパケットに対しては P I D 2 1 1 である。第 2 の P I D が割り当てられたパケットを、第 1 の期間では暗号化方式 B を用いて暗号化し、次の 8 期間ではクリアに送信する。そして、期間 1 0 において、上述した 4 つの P I D のいずれかを有するパケットを再び暗号化し、続く 8 期間ではクリアに送信する。同様に、第 1 のビデオ P I D 1 0 2 及び第 1 のオーディオ P I D 2 0 1 を有する番組 2 を、期間 2 において、暗号化方式 A を用いて暗号化し、対応する第 2 の P I D が割り当てられたパケットを、暗号化方式 B を用いて暗号化し、次の 8 期間ではクリアに送信し、以下同様とする。このパターンは、表 3 の最初の 9 行から明らかである。この技術によって、本発明を逸脱することなく、オーディオパケットとビデオパケットの両方を、オーディオパケットのみを、或いはビデオパケットのみを暗号化することができる。また、オーディオパケットとビデオパケットは、それぞれ個別の暗号化シーケンスを有することができる。表 3 において、P 1 は期間 1、P 2 は期間 2 を示し、以下同様である。E A は、情報が C A 方式 A を用いて暗号化されることを示し、E B は、情報が C A 方式 B を用いて暗号化されることを示す。

10

20

【 0 0 3 9 】

【表 3】

番組	ビデオ PID	オーディオ PID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	...
1	PID 101	PID 201	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	...
2	PID 102	PID 202	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
3	PID 103	PID 203	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
4	PID 104	PID 204	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
5	PID 105	PID 205	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
6	PID 106	PID 206	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	...
7	PID 107	PID 207	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	...
8	PID 108	PID 208	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	...
9	PID 109	PID 209	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	...
1	PID 111	PID 211	EB									EB			...
2	PID 112	PID 212		EB									EB		...
3	PID 113	PID 213			EB									EB	...
4	PID 114	PID 214				EB									...
5	PID 115	PID 215					EB								...
6	PID 116	PID 216						EB							...
7	PID 117	PID 217							EB						...
8	PID 118	PID 218								EB					...
9	PID 119	PID 219									EB				...

10

20

30

40

【 0 0 4 0 】

従来の旧式の暗号化方式（暗号化方式 A）と互換性を保つために、暗号化期間では、各

50

番組 1 ~ 9 を暗号化方式 A を用いて暗号化する。旧型の S T B 装置は、このように部分暗号化された A / V データストリームを受信し、透過的に、暗号化されていないパケットを通過し、暗号化されているパケットを復号する。しかしながら、暗号化方式 A と暗号化方式 B の両方を用いたデュアル暗号化方式の方が望ましい。デュアル暗号化を行うために、特定の有料番組には、第 1 の P I D (例えば番組 1 に対してはビデオ P I D 1 0 1 及びオーディオ P I D 2 0 1) と第 2 の P I D (例えば番組 1 に対してはビデオ P I D 1 1 1 及びオーディオ P I D 2 1 1) の両方が割り当てられ、特定の有料チャンネルのエレメンタリデータストリーム (elementary data stream) が送信される。

【 0 0 4 1 】

図 3 は、システム 2 0 0 におけるケーブルシステムヘッドエンド 2 2 2 の機能 (functionality) を概略的に示すブロック図であり、ヘッドエンド 2 2 2 において、N チャンネルのクリアなビデオパケット 2 0 4 は、インテリジェントスイッチ 2 1 6 (プログラミングされたプロセッサの制御下で動作する) に供給され、インテリジェントスイッチ 2 1 6 は、クリアに伝送するパケットを P I D 割当器 2 2 0 に供給し、P I D 割当器 2 2 0 は、これらのパケットに第 1 の P I D を割り当てる。暗号化されるパケットは、C A 方式 A 暗号化器 2 1 8 と C A 方式 B 暗号化器 2 2 4 の両方に供給される。C A 方式 A 暗号化器 2 1 8 と C A 方式 B 暗号化器 2 2 4 は、これらのパケットをそれぞれ暗号化して、P I D 割当器 2 2 0 に供給し、P I D 割当器 2 2 0 は、それぞれ第 1 の P I D 又は第 2 の P I D を割り当てる。クリアなパケット、C A 方式 A の暗号化パケット、C A 方式 B の暗号化パケット、システム情報 2 2 8 は多重化又は組み合わせられ、ケーブルシステム 3 2 を介して放

10

20

【 0 0 4 2 】

説明のために、タイムスライスの期間を 1 0 0 m s とすると、表 3 に示すように、平均して 1 . 1 (one and a fraction) の暗号化期間があり、合計して全 9 番組について毎秒 1 1 1 m s となる。タイムスライスの期間を 5 0 m s とすると、平均して 2 . 1 の暗号化期間があり、合計して 1 1 1 m s となる。未加入のセットトップボックスで、ビデオ信号に選局しようとした場合、如何なる画像に固定できたとしても、非常に悪い画質の画像しか得られず、音声は不明瞭なものとなってしまふ。

【 0 0 4 3 】

部分スクランブルされたストリームの P S I は、上述した具体例のデュアルオーディオ暗号化における場合と僅かに異なって処理される。基本的には、旧型のセットトップボックスと非旧型のセットトップボックスの両方に、同じ S I 及び P A T の P S I 情報を送信することができる。異なるのは、P M T の P S I 情報である。旧型のセットトップボックスは、P M T の P S I を解析して、従前の第 1 のビデオ P I D 及びオーディオ P I D を得る。非旧型のセットトップボックスは、旧型のセットトップボックスと同様に第 1 の P I D を得るが、データストリームが部分的にスクランブルされているか否かを確認するために、P M T の P S I 内の C A 記述子を調べなければならない。特定の C A プロバイダは、第 2 の P I D を故意にスクランブルしており、したがって、その P I D を送るためには、特定の C A プロバイダ固有の C A 記述子を用いる。本発明では、2 つ以上の第 2 の P I D を用いることができるようにすることによって、複数の C A プロバイダを共存させること

30

40

【 0 0 4 4 】

第 2 の P I D を、E C M で用いられているのと同じ C A 記述子内のプライベートデータとして送信できるが、好ましい実施例においては、別の C A 記述子を用いる。第 2 の P I D は、C A P I D フィールド内に配置されている。これにより、ヘッドエンド処理装置は、C A 記述子のプライベートデータフィールドを解析することなく、P I D を「調べる (see) 」ことができる。E C M の C A 記述子と第 2 の P I D の C A 記述子との違いは、第 2 の P I D の C A 記述子では、ダミーのプライベートデータ値を送信することができる

50

ことである。

【 0 0 4 5 】

【 表 4 】

<p>PID=0x0010 で伝送される PMT</p>	
<p>PMT 0x0010</p>	
- PMT 番組番号 1	
- PMT セクションバージョン 1 0	
- PCR PID 0x0011	
- エレメンタリストリーム	10
- ストリームタイプ (ビデオ 0x02 又は 0x80)	
- エレメンタリ PID (0x0011)	
- 記述子	
- CA プロバイダ # 1 用の CA 記述子(ECM)	
- CA プロバイダ # 2 用の CA 記述子(ECM)	
- CA プロバイダ # 2 用の CA 記述子(第 2 の P I D)	
- エレメンタリストリーム	
- ストリームタイプ (オーディオ 0x81)	
- エレメンタリ PID (0x0012)	
- 記述子	20
- CA プロバイダ # 1 用の CA 記述子(ECM)	
- CA プロバイダ # 2 用の CA 記述子(ECM)	
- CA プロバイダ # 2 用の CA 記述子(第 2 の P I D)	

【 0 0 4 6 】

【 表 5 】

CA プロバイダ # 2 用の CA 記述子(ECM)

記述子	30
- タグ : 限定受信 (0x09)	
- 長さ : 4 バイト	
- データ	
- CA 方式 ID : 0x0942 (第 2 の CA プロバイダ)	
- CA PID (0x0015)	

【 0 0 4 7 】

【表 6】

CA プロバイダ # 2 用の CA 記述子(第 2 の P I D)

記述子

- タグ : 限定受信 (0x09)
- 長さ : 5 バイト
- データ
 - CA 方式 ID : 0x1234 (第 2 の CA プロバイダ)
 - CA PID (0x0016)
 - プライベートデータ

10

【 0 0 4 8 】

CA 方式 A に基づいて動作する旧型の STB 36 は、データを受信すると、第 2 の PID を無視し、CA 方式 A によって暗号化されたパケットを復号し、テレビジョン受信機 44 に番組を表示する。非旧型の、すなわち新型の STB 236 は、SI 228 を受信する。新型の STB 236 は、PSI 229 を受信し、PMT を用いて、第 2 の CA 記述子内から読み出され、視聴する番組に関連した第 1 及び第 2 の PID を識別する。CA 方式 A によって暗号化されたパケットは破棄され、CA 方式 B によって暗号化され、第 2 の PID を有するパケットは、CA 方式 B 240 によって復号され、デコード及びテレビジョン受信機 244 に表するために、クリアなデータストリーム内に挿入される。

20

【 0 0 4 9 】

図 4 は、本発明の実施例を実現するために用いることができるケーブルシステムのヘッドエンドにおけるエンコード処理を示す図であり、CA 方式 A は、旧式の方式であり、CA 方式 B は、導入される新しい方式である。ステップ 250 において、所定の番組がクリアなパケットとして供給されると、そのパケット（又はフレーム）が暗号化されない（すなわち、暗号化の現在のタイムスライスが、この番組に対するものでない）ときは、ステップ 254 において、クリアなパケット（C）は、出力ストリームに挿入される。現在のパケットが、暗号化タイムスライスの一部であることにより暗号化される際には、パケットは、パケット暗号化処理 A のステップ 258 とパケット暗号化処理 B のステップ 262 において、それぞれ暗号化される。ステップ 258 における暗号化処理 A（EA）で暗号化されたパケットは、ステップ 254 において、出力ストリームに挿入される。ステップ 262 における暗号化処理 B（EB）で暗号化されたパケットは、ステップ 264 において、第 2 の PID が割り当てられ、ステップ 254 において、出力ストリームに挿入される。この処理が番組内の全てのパケットに対して繰り返される。

30

【 0 0 5 0 】

図 5 は、新たに導入された CA 方式 B を有する STB 236 において用いられる、上述した第 1 及び第 2 の PID を有する C パケット、EA パケット及び EB パケットを含む受信データストリームを復号及びデコードする処理を示す。ステップ 272 において、パケットが受信されると、そのパケットに所定の第 1 の PID があるか否かが調べられる。第 1 の PID がないときには、ステップ 274 において、そのパケットに所定の第 2 の PID があるか否かが調べられる。第 1 の PID と第 2 の PID のいずれもないときには、このパケットは、ステップ 278 において、無視或いは破棄される。第 1 の PID 又は第 2 の PID でない EA パケットと EB パケット間の如何なるパケットも、破棄される。デコーダが、常に EB パケットを受信する前に EA パケットを受信し、又は常に EA パケットを受信する前に EB パケットを受信することができるかは、設計事項及びバッファリングの問題である。また、第 2 のパケットを、第 1 のパケットの後ではなく前に検出するように設計することは、同様に容易である。また、第 2 のパケットを第 1 のパケットの前又は後のいずれにおいても受信できるように、回路を設計することは可能である。パケットに

40

50

所定の第1のPIDがある場合、ステップ284において、パケットが暗号化されているか否かが判定される。暗号化されていない場合、そのパケット(C)は、ステップ288において、直ちにデコーダに供給され、デコードされる。ステップ284においてパケットが暗号化されていると判定された場合、そのパケットは、EAパケットであるとみなされ、ステップ278において、破棄或いは無視される。ある実施例において、第1のパケットの暗号化は、ステップ284において調べない。むしろ、ステップ284において、第1(第2)のパケットの第2(第1)のパケットに対する位置を単に検出して、第1(第2)のパケットを識別することもできる。

【0051】

ステップ274において、パケットが第2のPIDを有する場合、第2のPIDは、ステップ292において、第1のPIDに再マッピングされる(或いは、同等に、第1のPIDは、第2のPID値に再割当てされる)。そして、パケットは、ステップ296において復号され、ステップ288においてパケットデコーダに供給され、デコードされる。言うまでもないが、本発明から逸脱することなく、様々の変更が可能であることは、当業者に明らかであり、例えば、ステップ292とステップ296の順番又はステップ272とステップ274の順番は入れ替えることができる。先に述べたように、ステップ284は、第2のパケットに対する第1のパケットの位置の検出に置き換えることができる。当業者は、他の変更を想到することもできる。

【0052】

暗号化方式Aによって動作する旧型のSTB36は、第2のPIDのパケットを完全に無視する。第1のPIDを有するパケットは、必要に応じて復号され、クリアなパケットのときは、復号されずにデコーダに供給される。したがって、暗号化方式Aによって動作する所謂「旧型の」STBは、第1のPIDに関連した部分暗号化データストリームを適切に復号及びデコードし、第2のPIDのデータストリームを変更することなく、無視する。暗号化方式Bによって動作するSTBは、第1のPIDに関連した全ての暗号化パケットを無視し、特定のチャンネルに関連した第2のPIDを有する、伝送されてきた暗号化パケットを用いるようにプログラミングされている。

【0053】

したがって、各デュアル部分暗号化された番組は、2セットのPIDを有する。暗号化が、上述のように適切なタイムスライス間隔によって示されるシステムに対して期間ベースで実行されるときには、いずれの復号方式も有さないSTBでは、画像は基本的に見ることができない。

【0054】

図6に示すヘッドエンド322においてこのシステムを実現するために、SI及びPSIは、CA記述子情報の第2のセットを含むように変更することができる。旧型のSTBは、未知のCA記述子を許容することができない。したがって、代わりに、旧型のSTBにおいて、コンテンツPID及び/又はSI/PSIと、ECMのPIDとの両方に対して、旧式CA PIDからのオフセットを「ハードコーディング(hard code)」することができるようにしてもよい。或いは、パラレルPSIを送ってもよい。例えば、非旧型のSTBに対しては、PID0ではなく、PID1000で補助的なPATを配信することができる。非旧型のSTBは、旧PAT内にはない補助的なPMTを参照することができる。補助的なPMTは、非旧式のCA記述子を含むことができる。補助的なPMTは、旧型のSTBには知られていないので、同時に使用(interoperation)の問題は生じない。

【0055】

モトローラ社又はサイエンティフィックアトランタ社によって製造された旧型のSTBに対応した方式Aのシステムにおいては、STBは何ら変更する必要はない。一方、方式B対応のSTBにおいては、ここに説明する部分暗号化された番組のデュアルキャリアジに対して、ビデオ及びオーディオデコーダは、それぞれ1つのみではなく、それぞれ2つのPID(第1のPID及び第2のPID)を参照する(listen)。使用する新CA方式の数によって、1つ以上の第2のシャドウPID(shadow PID)があるが、特定のSTB

10

20

30

40

50

は、そこに用いられているCA方式に適した1つの第2のPIDしか参照(listen)しない。また、ほとんどがクリアなビデオデータ又はクリアなオーディオデータを伝送している(carrying)PIDからの暗号化パケットは無視することが理想的である。「不適合パケット(bad packets)」（そのまま簡単にデコードできないパケット）は無視することは、多くのデコーダにおいて既に実行されている機能であるので、変更の必要はない。不適合パケットを無視しないデコーダを用いたシステムにおいては、フィルタ機能を用いることができる。なお、タイムスライス暗号化技術は、ビデオデータ及びオーディオデータにしか適用することができない。また、上述の実施例に示したように、ビデオデータはタイムスライス暗号化され、一方、オーディオデータはデュアル暗号化される。タイムスライス暗号化技術は、複数の番組に同時に適用することができる。ある期間に暗号化される番組の数は、帯域幅の割当てによって異なり、ここでは一度に1つの番組をスクランブルする例を記載しているが、本発明はこれに限定されるものではない。本明細書に記載の暗号化技術の他の組合せも、当業者に明らかである。

10

【0056】**M番目Nパケット暗号化**

本発明の他の実施例として、「M番目Nパケット暗号化(Mth & N packet encryption)」を説明する。これは、図3にシステム200として示す実施例の変形例である。この実施例では、それぞれ1つの番組を表すPIDのパケットは、ユーザが番組の料金を払っていない場合には、ユーザが番組を視聴できないように暗号化する。この実施例において、Mは、各暗号化イベント(event)の開始点間にあるパケットの数を表し、Nは、暗号化が一度開始してから連続して暗号化されるパケットの数を表す。NはMよりも小さい数である。M=9且つN=1ならば、9パケット毎に1パケット連続した暗号化イベントがある。M=16且つN=2ならば、16パケット毎に2パケット連続した暗号化イベントがある。上述の実施例のように、デュアル部分暗号化される各パケットは、CA方式A218及びCA方式B224を用いて複製及び処理される。この実施例と上述のタイムスライス暗号化技術との動作における違いは、スイッチ216の動作によって、プログラミングされたプロセッサの制御下で暗号化するパケットを選択することにある。

20

【0057】

本発明は、これに限定されるものではないが、この実施例によってデュアル暗号化される9チャンネルの番組を有するシステムを説明する。これらの9個のチャンネルは、9個の番組の内の特定の1番組に対応するパケットを識別するパケット識別子(PID)を用いてデジタル符号化される。この具体例では、これらの9個の番組は、番号101~109のビデオPID及び番号201~209のオーディオPIDを有することとする。この実施例における暗号化は、番組間でランダム(random program-to-program)であり、他の番組からのパケットを同時に暗号化してもよい。この具体例は、M=6且つN=2であり、ビデオパケットのみを暗号化する例である下表7に示されるが、これは本発明を限定するものではない。この方法は、コンテンツウェアである必要はない。表7において、PK1はパケット番号1を表し、PK2はパケット番号2を表し、以下同様である。

30

【0058】

【表 7】

番組	ビデオ	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
1	PID 101	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	...
2	PID 102	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	...
3	PID 103	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	...
4	PID 104	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	...
5	PID 105	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	...
6	PID 106	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	...
7	PID 107	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	...
8	PID 108	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	...
9	PID 109	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	...
1	PID 111	EB	EB					EB	EB					...
2	PID 112				EB	EB					EB	EB		...
3	PID 113			EB	EB	EB				EB	EB			...
4	PID 114				EB	EB					EB	EB		...
5	PID 115			EB	EB					EB	EB			...
6	PID 116	EB					EB	EB					EB	...
7	PID 117	EB	EB					EB	EB					...
8	PID 118		EB	EB					EB	EB				...
9	PID 119	EB					EB	EB					EB	...

10

20

30

40

【 0 0 5 9 】

表 7 に示す具体例では、各番組は、 $M = 6$ 且つ $N = 2$ の暗号化方式を用いて他の番組から完全に独立して暗号化される。ここでも、ビデオパッケージのみを暗号化する例を示しているが、この実施例又は他の変形例において、オーディオパッケージも暗号化してもよい。ビデオパッケージのみにこの暗号化を適用した場合、オーディオパッケージは、上述の実施例と同様に、デュアル暗号化又はタイムスライス暗号化してもよい。或いは、オーディオパ

50

ケットのみにこの暗号化を適用する場合、ビデオケットは、上述の実施例と同様に、タイムスライシングしてもよい。

【0060】

本明細書に開示する部分スクランブルの概念に対応する技術を様々に変形できることは当業者には明らかである。例えば、5個のクリアなケットの次に2個の暗号化ケット、2個のクリアなケット、1個の暗号化ケットと続くパターン(C C C C C E E C C E C C C C C E E C C E . . .)は、本発明の部分暗号化概念の変形例であり、暗号化するケットの選択のために、M及びNのランダム値、疑似ランダム値又はセミランダム値を用いてもよい。ケットのランダム、疑似ランダム又はセミランダム(ここでは全てを含めて「ランダム」という。)に選択することにより、ハッカーが、ポストプロセッシング(post processing)において、ケットをアルゴリズム的に再構築して、記録されたスクランブルコンテンツを再生することが困難になる。後述する部分暗号化の他の実施例にこの情報を適用する手法は、当業者に明らかである。幾つかの実施例は、組み合わせることで、コンテンツの安全性をより高めることができる。

10

【0061】

データ構造暗号化

本発明の実施例である他の部分暗号化方法では、データ構造毎に暗号化を行う。例えば、暗号化を好適に適用できるデータ構造の1つは、MPEGビデオフレームであるが、これに限定されるものではない。この具体例は、表8に示す具体例では、ビデオフレームを10フレーム毎に1フレーム暗号化する(ここでも、ビデオフレームのみを暗号化する)が、これは本発明を限定するものではない。この実施例では、各番組の10フレーム毎の暗号化サイクルは、それぞれのチャンネル毎に別個であるが、これは本発明を限定するものではない。この概念は、ビデオフレーム又はオーディオフレーム(或いは他の何らかのデータ構造)を基礎とし、例えばM=10且つN=1である、タイムスライシング又はM番目N部分暗号化配列(又は他のパターン)の変形例である。勿論、M及びNの他の値も同様の実施例において用いることができる。表8において、F1はフレーム番号1、F2はフレーム番号2を表し、以下同様である。

20

【0062】

【表 8】

番組	ビデオ	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
1	PID 101	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
2	PID 102	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
3	PID 103	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
4	PID 104	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
5	PID 105	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
6	PID 106	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
7	PID 107	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
8	PID 108	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
9	PID 109	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
1	PID 111	EB										EB		...
2	PID 112				EB									...
3	PID 113			EB										...
4	PID 114					EB								...
5	PID 115													...
6	PID 116	EB										EB		...
7	PID 117		EB										EB	...
8	PID 118		EB										EB	...
9	PID 119	EB										EB		...

10

20

30

40

【 0 0 6 3 】

したがって、ここでも、暗号化された番組は、それぞれ対応する2セットのPIDを付加されている。暗号化が上述のように、図に示すシステムに対して期間毎に実行された場合、画像は基本的に見ることができない。1秒間に30フレームを表示する9番組方式(nine program system)では、1秒間におよそ3フレームを暗号化する。番組視聴の権利を有さない視聴者のSTBが継続的に同期及び再生を試みても、部分的な静止画像を取得

50

することしかできない。番組視聴に加入している視聴者は、容易に番組を視聴することができる。このような暗号化構成の帯域幅使用量 (bandwidth cost) は、暗号化を適用する周波数帯域に依存する。上述の具体例では、各番組についてデータの 1 / 9 の追加的ファクタ (extra factor) が伝送される。この具体例では、およそ 1 番組相当の帯域幅が使用されている。番組数を多くすると、番組毎に暗号化されるパケット数は減り、暗号化システムのセキュリティは若干劣化する。ランダム化された M 番目 N パケット暗号化方式と同様に、ランダムフレームを選択してもよい。ビデオフレームの場合、ランダムフレームを選択することにより、全てのフレームタイプがアフェクトドイントラ符号化フレーム (affected-intra-coded frame: I フレーム)、前方予測符号化フレーム (predictive-coded frame: P フレーム)、両方向予測符号化フレーム (bi-directional-coded frame: B フレーム) 及び DC フレームであることを保証する。

10

【 0 0 6 4 】

本発明の変形例において、暗号化するパケットの数を更に減らしても、許容範囲のセキュリティレベルを達成できる。すなわち、例えば 9 番組方式においては、1 秒間に 1 つのフレームを暗号化するだけで、許容範囲のセキュリティレベルを達成できる。このような方式では、オーバーヘッドは、1 番組につき 1 秒間に 1 暗号化期間となり、すなわち、オーバーヘッドにおいて約 1 / 3 0 のデータが伝送される。このようなオーバーヘッドの削減は、2 つの暗号化方式によるフルデュアルキャリッジに対応した帯域幅の 5 0 % の伝送損失に比べると、著しい改善であると言える。本発明の他の変形例として、任意のビデオフレームのみを暗号化しても、許容範囲のセキュリティレベルを達成できる。例えば、M P E G コンテンツについて、I フレームだけをスクランブルすることにより、許容範囲のセキュリティレベルを維持したまま、帯域幅のオーバーヘッドを更に減少させることができる。これにより、フルデュアルキャリッジに必要な帯域幅を著しく削減することができる。

20

【 0 0 6 5 】

重要なパケットの暗号化

選択的なパケット毎のデュアル暗号化技術を用いることにより、帯域幅使用効率を大幅に高めることができる。このデュアル暗号化技術では、適切な番組コンテンツのオーディオ及び / 又はビデオデータに対する重要性に基づき、暗号化するパケットを選択する。

【 0 0 6 6 】

この実施例では、パケットの小さな部分のみをスクランブルすることによって、暗号化コンテンツのフルデュアルキャリッジに比べ、帯域幅使用量を減少させることができる。クリアなパケットは、2 個以上のデュアルキャリッジ P I D 間で共有される。好ましい一実施例において、後述するように、コンテンツ帯域幅全体の約 1 % 未満を使用する。旧暗号化方式のシステムにおいて、暗号化していない番組コンテンツパケットは、旧型及び新型の両方のセットトップボックスによって受信することができる。上述のように、暗号化パケットは、二重に伝送され (dual carried)、それぞれのセットトップボックスによって適切な C A 方式で処理される。各 C A 方式は、直交している。各 C A 方式において、鍵の共有は不要であり、新旧異なる鍵が用いられていてもよい。例えば、モトローラ社所有の暗号化方式は、組込みセキュリティ A S I C によって高速変更暗号鍵 (fast changing encryption keys) を発生させることができ、一方、N D S 社のスマートカードベースのシステムでは、それより僅かに遅い変更暗号鍵を生成する。この実施例は、サイエンティフィックアトランタ社及びモトローラ社の旧式の暗号化方式に対しても同等にうまく動作する。

30

40

【 0 0 6 7 】

図 6 は、本発明の一実施例として、番組の一部をパケット毎にデュアル暗号化するシステム 3 0 0 のブロック図を示している。このシステム 3 0 0 において、各番組のパケットは、例えば旧式の C A 方式 A と C A 方式 B を用いてデュアル暗号化される。暗号化されるパケットは、その重要度を基準に選択され、ビデオ及び / オーディオストリームの適切なデコーダに送られる。

【 0 0 6 8 】

50

図6に示すシステム300では、ケーブルシステムのヘッドエンド322は、パケット選択器316においてA/Vコンテンツ304の暗号化されるパケットを選択する。暗号化されるパケットは、それらが(料金未払いのデコーダによって)受信不能であることが、番組の実時間復号及び記録されたコンテンツのあらゆるポストプロセッシングに対して大きく影響するように選択される。すなわち、重要な(critical)パケット(以下、クリティカルパケットという。)のみが暗号化される。ビデオパケット及びオーディオパケットに対して、クリティカルパケットの暗号化は、PES(パケット化エレメンタリストリーム(packetized elementary stream))ヘッダ及びペイロードの一部としての他のヘッダを含む「フレーム開始(start of frame)」トランスポートストリームパケットを暗号化することにより達成することができる。これらの情報がなければ、STBのデコーダは、MP EG圧縮データを伸張することができない。MP EG2ストリームは、トランスポートヘッダ内の「パケット単位開始インジケータ(packet Unit Start Indicator)」によって「フレーム開始」パケットを識別する。一般的に、GOPヘッダ又はビデオシーケンスヘッダを含むペイロードを伝送するパケットを用いることによって、このスクランブル技術を実現することができる。

【0069】

MP EG(Moving Pictures Expert Group)方式に準拠した圧縮ビデオデータは、エレメンタリデータストリームを188バイトのデータを含むある程度(somewhat)任意のペイロードのトランスポートストリームに再パッケージ化する。このように、PESヘッダを含むトランスポートストリームパケットは、パケット選択器316において暗号化されるものとして選択され、CA方式A暗号化器318とCA方式B暗号化器324の両方によってデュアル暗号化される。デュアル部分暗号化されるパケットは、複製され、暗号化器324によって暗号化され、複製されたパケットのPIDは、上述の実施例と同様に、第2のPID割当器330において第2のPIDに割り当てられる。残りのパケットは、クリアなまま渡される。クリアなパケットと、CA方式Aによって暗号化されたパケットと、CA方式Bによって暗号化されたパケットと、システム情報328とは、互いに多重化され、ケーブルシステム32を介して放送される。

【0070】

上述した方式と同様に、旧型のSTB36は、クリアなデータ及びCA方式Aによって暗号化されたデータを受信し、CA方式A40によって復号されたデータと暗号化されていないデータを組み合わせてトランスペアレントにSTB36のデコーダに供給する。新型のSTB336において、番組は、第1のPID及び第2のPIDの両方に割り当てられている。第1のPIDを有するクリアなパケットは、受信されてデコーダに供給される。第1のPIDを有する暗号化されたパケットは、除外(discarded)される。第2のPIDを有する暗号化されたパケットは、復号されて、デコードのために、(例えば、パケットを第1のPIDに再マッピングすることによって)データストリームに再挿入される。

【0071】

ビデオデータを具体例として説明すると、各サンプルは、フレームと呼ばれ、サンプリングレートは、通常、30フレーム毎秒である。3.8Mbpsに適合するようにサンプルを符号化する場合、各フレームは、帯域幅のうちの127kビットを占有する。MP EGトランスポートのデータは、188バイトのパケットに分割(sliced)され、各フレームの第1のパケットは、フレームデータの本体の処理を指示するために用いられるヘッダを含んでいる。第1のヘッダパケットのみ(追加的な1504ビット)をデュアル暗号化する場合、必要となる追加的な帯域幅は、1.2%(1504/127k)のみである。高精細度(high definition)ストリーム(19Mbps)の場合、この割合は更に小さくなる。

【0072】

上述のように、本発明の実施例においては、PESヘッダを含むトランスポートストリームパケットを暗号化の対象とすることが望ましい。これらのパケットは、シーケンスヘ

10

20

30

40

50

ッダ (sequence header) と、シーケンス拡張ヘッダ (sequence extension header) と、ピクチャヘッダと、同じパケット内にも含まれる量子化及び他のデコードテーブルとを含んでいる。これらのパケットをデコードできない場合、(すなわち、ハッカーが加入料を払わないで、許可されていない番組を視聴しようとした場合)、番組の大部分が視聴できない。多くの場合、番組を選局しようとして、ブランク画面が表示されるだけであり、周知のデコーダ集積回路は、PESヘッダを用いて、ビデオ及びオーディオ等のエレメンタリストリームを実時間で同期させているため、音声も聞こえない。PESヘッダを暗号化することにより、未許可のセットトップボックス内のデコードエンジンは、動作を開始することすらできない。例えば保存されたコンテンツに対するポストプロセッシング攻撃 (post processing attacks) は、PESヘッダを含むパケット内のクリティカルな動的に変化する情報 (critical dynamically changing information) によって防がれる。本発明の主旨から逸脱することなく、未許可の視聴を防止するために、この他のクリティカルな、すなわち重要なパケット、又はコンテンツ要素を暗号化してもよいことは当業者にとって明らかである。例えば、MPEGイントラ符号化フレーム、すなわちIフレームピクチャパケットを暗号化して、番組のビデオ部分の視聴を制限してもよい。本発明の実施例は、他の如何なる実施例と組み合わせてもよく、例えば、PESヘッダを含むパケットを暗号化するとともに、他のパケットに対してランダム暗号化、M番目N暗号化、又はデータ構造暗号化を施してもよい。クリティカルパケット暗号化を用いてビデオデータを暗号化し、他の暗号化方式をオーディオデータに適用してもよい。オーディオデータは、例えば、デュアル暗号化してもよい。当業者は、本発明の範囲内で様々な変形例を想到することができる。

10

20

30

40

50

【0073】

図7は、例えば図6に示すヘッドエンド322に適用される具体的な符号化処理を説明するフローチャートである。トランスポートストリームパケットを受信すると、ステップ350において、パケットを調べ、このパケットが暗号化のための選択基準 (selection criteria) を満たすか否かを判定する。好ましい実施例においては、選択基準は、パケットペイロードの一部としてPESヘッダが存在していることである。この選択基準を満たさない場合、パケットは、クリアな、暗号化されていないパケット (C) として渡され、ステップ354において、出力データストリームに挿入する。パケットがこの選択基準を満たす場合、ステップ358において、このパケットをCA暗号化方式Aで暗号化し、暗号化されたパケットEAを生成する。更に、このパケットを複製し、ステップ362において、複製されたパケットをCA暗号化方式Bで暗号化し、暗号化されたパケットを生成する。ステップ366において、この暗号化されたパケットを第2のPIDにマッピングし、これにより、暗号化されたパケットEBを生成する。ステップ354においては、暗号化されたパケットEA、EBをクリアなパケットCとともに、出力データストリームに挿入する。好ましくは、暗号化されたパケットEA、EBは、データストリームにおいて、元の単一のパケットが暗号化のために取り出された位置に挿入し、データのシーケンスが基本的に同じになるようにするとよい。

【0074】

ステップ354において生成された出力データストリームが、例えば図6に示すSTB336等のCA暗号化方式Bに準拠したSTBによって受信されると、図8 (図5に類似している。) に示すような処理により、番組を復号及びデコードする。第1のPID又は第2のPIDを有するパケットが受信されると、ステップ370において、パケットがクリア (C) であるか、CA暗号化方式Aに基づいて暗号化されているか (EA) を判定し、ステップ374において、このパケットがCA暗号化方式Bに基づいて暗号化されているか (EB) を判定する。パケットがクリアである場合、このパケットをデコーダ378に直接渡す。幾つかの実施例においては、第1 (第2) のパケットが第2 (第1) のパケットの前にあるか又は後ろにあるかといった相対的位置に基づいて、第1 (第2) のパケットをストリーム内で検出してもよい。この場合、第1のパケットのスクランブル状態を特に確認する必要はない。パケットがEAパケットである場合、ステップ380において

、このパケットを破棄する。パケット E B パケットである場合、ステップ 3 8 4 において、このパケットを復号する。この時点において、ステップ 3 8 8 において、第 2 の P I D パケット及び / 又は第 1 の P I D パケットを同じ P I D に再マッピングする。そして、デコード 3 7 8 において、復号されたパケット及びクリアなパケットをデコードする。

【 0 0 7 5 】

上述したデュアル部分暗号化方式によって、フルデュアルキャリッジの場合に比べて、帯域幅要求を大幅に削減することができる。P E S ヘッダ情報の暗号化は、ビデオ及びオーディオコンテンツの安全性を確保する点で有効であるとともに、これにより、同じケーブルシステム内に 2 つ以上の C A 方式を独立して「共存 (co-exist)」させることができる。この場合、旧型の A 方式のセットトップボックスには影響がなく、B 方式のセットトップボックスも、ビデオ及びオーディオデータについて 2 つの P I D を参照するよう、ハードウェア、ファームウェア又はソフトウェアを僅かに拡張すればよい。旧型及び非旧型の S T B は、それぞれの基本的な C A 方式を維持する。ヘッドエンドの変更は、暗号化するためのコンテンツを選択する点のみに限られ、すなわち、第 2 の暗号化器と、暗号化されたパケットと暗号化されていないパケットとを混合して合成出力ストリーム (composite output stream) を生成する回路とを設ければよい。

10

【 0 0 7 6 】

一実施例においては、ヘッドエンド装置は、状況に応じて、クリティカルな P E S ヘッダのみではなく、帯域幅が許す限り多くのコンテンツを暗号化する。これらの更なる暗号化されたパケットは、P E S ペイロード内のパケットであっても、ビデオ / オーディオフレームにおける他のパケットであってもよく、これにより、コンテンツの安全性が更に高められる。

20

【 0 0 7 7 】

S I 暗号化 (S I ENCRYPTION)

図 9 は、更なる帯域幅の必要性を最小化するシステム 4 0 0 の具体的構成を示している。この実施例では、システム 4 0 0 は、セットトップボックスにおいて、番組を選局するためには、システム情報 (S I) 4 2 8 が必要であるという事実を利用している。ケーブルシステムでは、S I は、帯域外 (out-of-band)、すなわち通常の視聴チャンネルの周波数以外の周波数で伝送される。また、S I は、帯域内 (in-band) で送信してもよい。帯域内で送信する場合、S I 4 2 8 は、各ストリームに対して複製され、各ストリームとともに送信される。説明のために、「旧型の」セットトップボックスに供給される S I が、例えば S T B 4 3 6 等の新しいセットトップボックスに供給される S I とが分離されているとする。これにより、S I 4 2 8 の各バージョンは、C A 方式 A 4 1 8 と C A 方式 B 4 2 4 を用いて個別に暗号化される。クリアなビデオデータ 4 0 4 及びクリアなオーディオデータ 4 0 6 は、クリアな形式で配信されるが、これがクリアであることを示すためには、S I 4 2 8 が必要である。

30

【 0 0 7 8 】

S I は、チャンネル名、及び例えばプログラム名、開始時刻等を含むプログラム案内情報等の情報とともに、各チャンネルの周波数選局情報 (frequency tuning information) を含んでいる。デジタルチャンネルは、互いに多重化され、特定の周波数を介して伝送される。本発明の実施例では、S I 情報は暗号化され、許可されたセットトップボックスのみで利用可能となる。システム (plant) 内の全ての A / V 周波数の割り当てを示す S I 情報が受信されなかった場合、選局を行うことはできない。

40

【 0 0 7 9 】

セットトップボックスを改造して、周波数の試行又はスキャンングを行おうとするハッキング行為を不能にするために、チャンネルの周波数を、標準的な周波数からオフセットさせてもよい。更に、日毎、週毎又はこの他の周期で、若しくはランダムに、周波数を動的に変更してもよい。一般的なケーブルシステムのヘッドエンドは、約 3 0 個の周波数帯域を用いる。各周波数は、多くの場合、相互の周波数間で、地上波放送信号との間で、及び受信装置のクロックとして用いられている周波数との間で干渉が生じないように、選択

50

される。各チャンネルは、使用されても干渉を生じず、若しくは使用されると隣接するチャンネルの周波数が変更される独立した少なくとも1つの代替周波数 (alternate frequency) を有する。したがって、実際に可能な周波数マップは、 2^{30} 又は 107×10^9 個となる。ここで、ハッカーは、単純に、各局の両方の周波数について、30個のチャンネルのそれぞれを試すような行為を行う可能性もある。コンテンツを提供する周波数の特定に成功すると、ハッカーのセットトップボックスは、PSI 429を解析し、番組を構成する個々のPIDに関する情報を得る。ここで、ハッカーが「番組1」が「CNN」の番組であり、「番組5」が「TNN」の番組である、といったことを特定することは困難である。このような情報は、上述のように暗号化され、未許可のセットトップボックスでは利用できないSIとともに送信されている。しかしながら、ハッカーが配信されたコンテンツのそれぞれを選択し、調べれば、番組と局の対応関係も把握することができる。このようなチャンネルの特定を妨害するために、単一のストリーム内の番組の割り当てを時刻によって変更し、例えば、上述した具体例における番組1と番組5とを入れ替え、「番組1」を「TNN」にし、「番組5」を「CNN」にするなどして、ハッカーを混乱させてもよい。或いは、全く新しい番組のグループ化に基づいて、番組を全く異なるストリームに移動させてもよい。一般的なケーブルシステムのヘッドエンドは、音楽番組を含む250個の番組のコンテンツを配信する能力を有する。それぞれの番組を固有に選局することができる。再順序付けの可能な組合せは $250!$ (階乗) 個である。配信されたSI又はハッカーのいずれかによって提供されたコンテンツのマップがなければ、ユーザは、番組をランダムに選局して、その番組に興味があるものであるか否かを確かめなくてはならなくなる。

10

20

【0080】

このように、ヘッドエンド422においては、ビデオ信号404及びオーディオ信号406がクリアな (暗号化されていない) 形式で供給され、SI 428は、複数のCA方式に基づき、ケーブルネットワークを介して配信される。したがって、この具体例に示すシステム400においては、クリアなSI 428は、暗号化器418に供給され、暗号化器418は、暗号化方式Aを用いてSIを暗号化する。同時に、クリアなSI 428は、暗号化器424にも供給され、暗号化器424は、暗号化方式Bを用いて、SIを暗号化する。次に、クリアなビデオ及びオーディオは、暗号化器418からの暗号化されたSI (SI A)、暗号化器424からの暗号化されたオーディオデータ (SI B)、帯域外システム情報428とともに多重化される。

30

【0081】

ケーブルシステム32を介して配信された後、ビデオデータ、オーディオデータ、システム情報A、システム情報Bは、全て、セットトップボックス36及びセットトップボックス436に供給される。STB36においては、暗号化されたSIは、CA方式A40において復号され、セットトップボックスに選局情報が提供される。セットトップボックス36は、特定の番組を選局し、テレビジョン受信機44に表示させる。同様に、STB436においては、暗号化されたSIは、CA方式B440において復号され、セットトップボックスに選局情報が提供され、これにより、特定の番組を選局し、テレビジョン受信機444に表示できるようになる。

40

【0082】

この手法により、例えばケーブルシステム等のコンテンツ配信システムにおいて、追加的なA/V帯域を用意する必要がなくなるという利点がある。ここでは、SIのみがデュアル伝送 (dual carried) される。特別なハードウェアも不要である。大部分のチューナは、標準周波数からの如何なるオフセット周波数にも容易に適応することができる。SI復号は、ソフトウェアによって実行してもよく、ハードウェアの助けを借りて行ってもよい。例えば、旧型のモトローラ社 (Motorola) のセットトップボックスは、デコーダ集積回路チップ内に組み込まれたハードウェア復号器を用いて、モトローラ帯域外周波数帯 (Motorola out-of-band) を介して配信されたSIを復号する能力を有する。

【0083】

50

ハッカーが同軸ケーブルにスペクトルアナライザを用いて、A/Vチャンネルを特定する可能性もある。更に、比較的時間がかかる処理であるが、ハッカーがセットトップボックスを改造して、周波数帯域を自動スキャンし、A/Vチャンネルを特定する可能性もある。A/Vチャンネル周波数を動的に変化させれば、ハッカーは、継続的に帯域を分析又はスキャンしなくてはならなくなり、このようなハッカーの行為を挫折させることができる。更に、プログラム番号及び割り当てられるPIDを変更してもよい。但し、周波数、プログラム番号、PIDを動的に変更すると、例えば、ケーブルシステムのオペレータ等のサービスプロバイダにおける処理が複雑になる。

【0084】

包括的表現 (GENERALIZED REPRESENTATION)

10

上述した各手法は、包括的に、図10のシステム500として表現することができる。このシステム500は、ケーブルシステムヘッドエンド522を備え、ケーブルシステムヘッドエンド522は、クリアなビデオデータ504と、クリアなオーディオデータ506と、SI528と、PSI529とを備え、これらは、インテリジェントプロセッサによって制御されたスイッチ518を介して選択的に切り換えられ、スイッチ518は、PIDの割当 (PID割当又は再割当を要求する実施例において) を行い、上述した各データを選択的に、CA方式A504又はCA方式B524に供給し、或いは、クリアな形式でケーブルシステム32に供給する。従来と同様、旧式のCA方式Aによって暗号化された番組又はSIは、STB36によって正しく復号される。CA方式Bによって暗号化された情報は、上述のように、STB536によって検出され、復号され、デコードされる。

20

【0085】

PIDマッピングに関する考察

上述したPIDマッピングの概念は、必要に応じて、ここに説明したデュアル部分暗号化方式に適用することができる。包括的には、ケーブルシステムのヘッドエンドにおいて、パケットのデータストリームは、暗号化のために選択されたパケットを複製するように操作される。これらのパケットは、複製され、2つの異なる暗号化方式に基づいて暗号化される。複製されたパケットには、個別のPID (これらのうちの1つは、クリアなコンテンツに用いられる旧型のCAのPIDに対応する) が割り当てられ、これらのパケットは、データストリームにおける元の選択されたパケットの位置に挿入され、ケーブルシステムを介して伝送される。ケーブルシステムのヘッドエンドからは、同じPIDを有する旧式の暗号化が施されたされたパケット及びクリアなパケットのストリームが出力される。第2のPIDは、パケットが新しい暗号化方式で暗号化されていることを示す。ヘッドエンドで行われるPID再マッピングに加えて、MPEGパケットは、連続カウンタ (continuity counter) を利用し、パケットの適切なシーケンスを維持する。適切な復号が行われることを保証するために、ヘッドエンドにおいて、パケット化されたデータストリームを生成する間、この連続カウンタを適切に維持する必要がある。これは、各PIDを有するパケットが、連続カウンタに通常の手法で連続的に割り当てられるようにすることで達成される。これにより、第2のPIDを有するパケットは、第1のPIDの連続カウンタからは、独立した連続カウンタを有することとなる。これを単純な形式で以下に示す。

ここでは、PID025は、第1のPIDであり、PID125は、第2のPIDであり、Eは、暗号化されたパケットを表し、Cは、クリアなパケットを表し、末尾の数字は、連続カウンタを表す。

30

40

【0086】

【表9】

025C04	025E05	125E11	025C06	025C07	025C08	025C09	125E12
--------	--------	--------	--------	--------	--------	--------	--------

【0087】

50

この例示的なパケットのセグメントでは、P I D 0 2 5 を有するパケットは、独自の連続カウンタのシーケンス (0 4 , 0 5 , 0 6 , 0 7 , 0 8 , 0 9 , . . .) を有する。同様に、第 2 の P I D 1 2 5 を有するパケットは、独自の連続カウンタのシーケンス (1 1 , 1 2 , . . .) を有する。S T B においては、P I D は、任意の数の手法で処理することができ、第 2 の P I D を有する暗号化されたパケットと正しい番組とが適切に関連付けられる。パケットヘッダを含む入力ストリームセグメントの一具体例を以下に示す。

【 0 0 8 8 】

【表 1 0】

025C04	025E05	125E11	025C06	025C07	025C08	025C09	125E10
--------	--------	--------	--------	--------	--------	--------	--------

10

【 0 0 8 9 】

この入力ストリームを処理することにより、次のような出力ストリームセグメントが生成される。

【 0 0 9 0 】

【表 1 1】

125C04	025E11	125E05	125C06	125C07	125C08	125C09	125E10
--------	--------	--------	--------	--------	--------	--------	--------

20

【 0 0 9 1 】

第 1 の P I D (0 2 5) は、入力ストリーム内のクリアなパケット (C) 用の第 2 の P I D (1 2 5) に置換される。暗号化されたパケットについては、第 1 の P I D 及び第 2 の P I D が維持されるが、連続カウンタが入れ替えられる。これにより、パケットのストリームは、第 2 の P I D を用いることによる継続性の喪失によるエラーを生じることなく正しく復号及びデコードできる。本発明の実施例とともに、P I D の処理に関する他の手法として、例えば、スクラプリングされた旧型のパケットの P I D (1 2 5) を N O P P I D (全てが 1) 又は復号されない他の P I D 値にマッピングしてもよく、連続カウンタを用いてもよい。

30

【 0 0 9 2 】

第 1 及び第 2 の P I D は、番組特定情報 (program specific information : P S I) データストリームの一部として伝送される放送番組マップテーブル (program map table : P M T) に含まれて S T B に供給される。第 2 の P I D の存在は、C A 暗号化方式 A (「旧式の」方式) に基づいて動作する S T B によっては無視することができ、一方、C A 暗号化方式 B に基づいて動作する新たな S T B は、第 2 の P I D が第 1 の P I D に関連する番組の暗号化された部分を伝送するために用いられていることを認識するようプログラミングされる。セットトップボックスには、P M T の基本 P I D 「フォーループ (for loop) 」における C A 記述子の存在によって、暗号化方式が用いられていることが知らされる。通常、ビデオ基本 P I D 「フォーループ」のための C A 記述子と、オーディオ基本 P I D 「フォーループ」のための他の C A 記述子とが存在する。C A 記述子 (CA descriptor) は、プライベートデータバイト (Private Data Byte) を用いて、C A _ P I D を E C M P I D 又は部分暗号化に用いる第 2 の P I D として識別し、これにより、S T B の動作を単一の番組に関連する第 1 及び第 2 の P I D を検出する方式 B に設定する。トランスポートヘッダ内の P I D フィールドは、13 ビット長であるため、 2^{13} すなわち 8192 個の P I D を使用することができ、必要に応じて、予備の如何なる P I D を第 2 の P I D として用いてもよい。

40

【 0 0 9 3 】

各番組コンポーネントに又は番組コンポーネントの選択された部分に P I D を割り当てることに加えて、第 2 の暗号化方式において用いるタグ E C M データに新たな P I D を割

50

り当ててもよい。割り当てられる各 P I D 番号は、旧型の S T B の動作に支障を生じさせないために、ユーザにより定義されたストリームタイプとして指定される。M P E G では、このような数の予備ブロックを、ユーザにより定義されたデータストリームタイプとして定義している。

【 0 0 9 4 】

ケーブルヘッドエンドにおける P I D マッピングは、概念的にも、単純な処理であり、実際に、ケーブルヘッドエンドの設備は、既にこのようなマッピングに対応しており、したがって、既存のケーブルシステムの最小限の変更で、低コストに、このような方式を実現することができる。ケーブルシステムヘッドエンド内において、この方式をどのように実現するかについては、後に具体例を挙げて詳細に説明するように、ヘッドエンド内の実際の旧型のハードウェアに依存する。

10

【 0 0 9 5 】

ヘッドエンドの実現

図 2、図 3、図 6、図 9、図 10 を参照して説明した上述の実施例は、ある程度概念的な性質を有し、本発明の様々な実施例に関連する全体的な発想及び概念を説明するために用いられていることは、当業者にとって明らかである。本発明を現実的に実現するためには、既に設立されているケーブルプロバイダの既存の旧型のヘッドエンド装置において、様々な部分暗号化方式について、コスト効率が高い実現が必要であるという現実世界での重要な問題があることは当業者にとって明らかである。ここでは、2つの旧型のケーブルシステムを具体例として、上述の手法をケーブルヘッドエンドにおいてどのように実現するかを説明する。

20

【 0 0 9 6 】

まず、モトローラ社の限定受信技術を用いたケーブルシステムヘッドエンドについて考察する。このようなシステムでは、デュアル部分暗号化を低コストで実現するために、図 11 に示すような変更を行うことができる。典型的なモトローラ方式であるヘッドエンドインザスカイ (Headend In The Sky : 以下、H I T S という。) 又は類似の方式では、信号は、衛星から供給される。この方式では、ケーブルプロバイダから提供され、例えば、モトローラ集積受信機トランスコーダ (Motorola Integrated Receiver Transcoder : I R T) モデル I R T 1 0 0 0 及び I R T 2 0 0 0 及びモトローラモジュラ処理システム (Motorola Modular Processing System : M P T) 等の受信機 / デスクランブラ / ス克蘭ブラシステム 6 0 4 に受信される集合的な (aggregated) デジタル化されたコンテンツを提供する。デジタルテレビジョンデータのクリアなストリームは、受信機 / デスクランブラ / ス克蘭ブラシステム 6 0 4 の衛星デスクランブラ機能ブロック 6 0 6 から得ることができる。このクリアなストリームは、パケット選択器 / デュプリケータ 6 1 0 として示す新たな機能ブロックによって処理される。このパケット選択器 / デュプリケータ 6 1 0 は、プログラミングされたプロセッサとして、又はハードウェア又はソフトウェア及びこれらの組合せとして実現できる。

30

【 0 0 9 7 】

パケット選択器 / デュプリケータ 6 1 0 は、上述したデュアル部分暗号化のうちのいずれかに基づいてデュアル暗号化すべきパケットを選択する。これらのパケットは、複製され、後の暗号化において特定できるように、新たな P I D が付される。例えば、パケット選択器 / デュプリケータ 6 1 0 に供給された特定の番組に関連するパケットが P I D 「 A 」を有する場合、パケット選択器 / デュプリケータ 6 1 0 は、そのパケットを暗号化すべきパケットであると識別し、これらのパケットを複製し、これらのパケットに P I D 「 B 」、P I D 「 C 」をそれぞれ再マッピングする。これにより、後の暗号化において、これらのパケットを異なる 2 つの方式に応じて特定することができる。好ましくは、複製されたパケットは、P I D 「 C 」とともに、互いに隣接して、データストリームの複製された元のパケットの位置に挿入される。これにより、これらのパケットは、元の位置を維持する (但し、元のデータストリームには 1 つのパケットしかなかった位置に 2 つのパケットが存在することとなる)。ここで、追加すべき新たな C A 方式が N D S 方式の暗号化であ

40

50

るとする。この場合、P I D「A」は、クリアなパケットを表し、P I D「B」は、N D S方式で暗号化されたパケットを表し、P I D「C」は、モトローラ方式で暗号化されたパケットを表す。P I D「B」を有するパケットは、この時点で、パケット選択器/デュプリケータ610において、N D S暗号化方式で暗号化してもよく、後に暗号化してもよい。

【0098】

P I D「B」及びP I D「C」を有するパケットは、受信機/デスクランブラ/スクランブラシステム604に戻され、ここで、P I D「C」を有するパケットは、モトローラ社の装置に関連する制御方式614に基づき、ケーブルスクランブラ612において、モトローラ暗号化方式で暗号化される。ケーブルスクランブラ612からの出力ストリームは、更なる新たな装置であるP I D再マッピング及びスクランブラ620に供給され、P I D再マッピング及びスクランブラ620は、ケーブルスクランブラ612から受け取ったデータについて、残りのパケットにP I D「A」乃至P I D「C」を再マッピングし、制御方式624による制御に基づき、N D S暗号化アルゴリズムを用いて、P I D「B」を有するパケットを暗号化する。出力ストリーム626は、P I D「C」を有するクリアな暗号化されていないパケットと、複製され、選択され、モトローラ暗号化方式によって暗号化されたP I D「C」を有するパケットと、複製され、選択され、N D S暗号化方式によって暗号化されたP I D「B」を有するパケットとを含む。このストリームは、ケーブルシステムを介して配信するために、(例えば、直交振幅変調(quadrature amplitude modulation: 以下、Q A Mという。))又はR F変調により)変調される。好ましい実施例では、旧型の番組特定情報(P S I)において用いられているオーディオ及びビデオP I Dとの互換性を保つために、P I D「A」が付された暗号化されていないパケットをP I D「C」が付されたスクランブルされたパケットに一致するようにマッピングする。制御コンピュータ、スクランブラ及び旧型のセットトップボックスは、P I D「C」に関する知識のみを有している。これに代えて、P I D「C」が付されたスクランブルされたパケットを逆にP I D「A」にマッピングしてもよいが、この場合、自動的に生成されたP S Iを編集して、P I D再マッピング及びスクランブラ620においてP I D「C」からのP I D番号をP I D「A」に振り直す必要がある。

【0099】

上述の実施例において、P I D再マッピング及びスクランブラ620は、P S I情報の複製に用いることもでき、この場合、P I D再マッピング及びスクランブラ620は、P S I情報を変更して、(P M TにおけるC A記述を用いて)N D S暗号化の追加を反映させ、変更したP S I情報をデータストリームに多重化して戻してもよい。更に、P I D再マッピング及びスクランブラ620において、N D S暗号化をサポートするE C Mをデータストリームに挿入してもよい(又は、パケット選択器/デュプリケータ610によってこれを挿入してもよい)。

【0100】

このように、N D S暗号化方式(又は、この他の暗号化方式)をモトローラ社の設備を用いるケーブルシステムヘッドエンドに追加するために、パケットが複製され、衛星デスクランブラからのデータストリームにおいてP I Dが再マッピングされる。再マッピングされたP I Dは、各C A方式に基づいてスクランブルすべきパケットを特定するために用いられる。旧式の暗号化方式を採用する場合、クリアなパケットのP I Dは、旧式の方式におけるクリアなパケットと暗号化されたパケットの両方が同じP I D(又は複数のP I D)を共有するように再マッピングされる。P I D再マッピング及びスクランブラ620におけるP I Dの再マッピング及びパケット選択器/デュプリケータ610におけるパケットの選択と複製は、プログラミングされたプロセッサ、若しくは、例えば特定用途向け集積回路等のカスタムの又はセミカスタムの集積回路、プログラマブルロジックデバイス又はフィールドプログラマブルゲートアレーを用いて実現してもよい。本発明の範囲から逸脱することなく、これらを別の手法で実現することもできる。

【0101】

図12は、サイエンティフィックアトランタ社のケーブルヘッドエンドにおいて、本発明に基づくデュアル部分暗号化を実現するために用いる同様の設備構成を示している。この実施例では、HITS信号又は同様の信号が衛星信号デスクランブラ706が組み込まれたIRD704において受信される。これは、衛星信号デスクランブラ機能がイネーブルにされたモトローラ社のIRT又はMPSであってもよい。衛星信号デスクランブラ706からの出力信号は、新たなパケット選択器/デブリケータ710によって処理できるクリアなデータストリームであり、パケット選択器/デブリケータ710は、パケット暗号化すべきパケットを選択し、これらを複製し、複製されたパケットのPIDを新たなPIDにマッピングする。ここでも、例えば、クリアなまま残すパケットには、PID「A」が割り当てられ、新たな方式(例えば、NDS)で暗号化すべきパケットには、PID「B」が割り当てられ、サイエンティフィックアトランタ社の方式で暗号化すべきパケットには、PID「C」が割り当てられる。パケットPID「B」が付されたパケットは、この時点で、NDS暗号化方式で暗号化される。

10

20

30

40

50

【0102】

パケットのストリームは、マルチプレクサ712(例えば、サイエンティフィックアトランタ社製マルチプレクサ)に供給され、マルチプレクサ712は、マルチプレクサ712に関連する制御方式718による制御の下、ケーブルスクランブラ714において、PID「C」を有するパケットをサイエンティフィックアトランタ暗号化方式で暗号化する。次に、データストリームは、マルチプレクサ712の内部でQAM変調器720に供給される。パケットを正しく再マッピングするために、マルチプレクサ712から出力されるQAM変調信号は、新たな処理部724に供給され、ここで、QAM変調信号は、QAM復調器730によって復調され、次に、PID再マッピング器734において、制御方式738による制御の下、クリアなPID「A」パケットがPID「C」に再マッピングされる。NDS暗号化アルゴリズムに基づく暗号化もパケット選択器/デブリケータ710ではなく、ここで実行される。PIDが再マッピングされ、デュアル部分暗号化されたデータストリームは、QAM及びRF変調器742によってQAM変調及び/又はRF変調された後、ケーブルシステムを介して配信される。

【0103】

上述の実施例においては、更に、PID再マッピング及びスクランブラ734を用いて、PSI情報の逆多重化し、PSI情報にNDS暗号化の付加を反映させ(PMTにCA記述子を追加する)、変更されたPSI情報をデータストリームに戻す。PID再マッピング及びスクランブラ734において、データストリームにNDS暗号化をサポートするためのECMを挿入してもよい(或いは、これをパケット選択器/デブリケータ710によって挿入してもよい)。PID再マッピング及びスクランブラ734におけるPID再マッピング及び/又はスクランブル、QAM復調器730及びQAM及びRF変調器742によるQAM復調及びQAM変調、及びパケット選択器/デブリケータ710におけるパケットの選択と複製は、プログラミングされたプロセッサ、若しくは、例えば特定用途向け集積回路等のカスタムの又はセミカスタムの集積回路、プログラマブルロジックデバイス又はフィールドプログラマブルゲートアレーを用いて実現してもよい。本発明の範囲から逸脱することなく、これらを別の手法で実現することもできる。

【0104】

本発明の上述の実施例により、旧型のスクランブル装置は、全てのエレメンタリストリームではなくエレメンタリストリームにおける望まれるパケットのみをスクランブルできる。任意のパケットの選択的なスクランブルは、エレメンタリストリームにおけるスクランブルする必要がないパケットに対し、例えば、PID「A」といった所定のPID番号を付すことによって実現する。スクランブルされるパケットには、例えば、PID「C」を付す。スクランブル装置は、PID「C」が付された(スクランブルすると選択された)パケットをスクランブルする。スクランブルが行われた後、スクランブルされていないパケットは、スクランブルされたパケットにマッピングされたPID番号と同じPID番号を有することとなり、PID「A」がPID「C」となる。旧型のセットトップボック

スは、スクランブルされたパケット及びスクランブルされていないパケットの両方とともにエレメンタリストリームを受信する。

【0105】

これらの実施例におけるパケットは、ストリームとして処理される。全体のストリームは、スクランブルのために旧型のスクランブル装置に供給される。これにより、全てのパケットが正確な時間同期順に保たれる。パケットがストリームから抽出され、旧型のスクランブル装置に供給されると、時間的ジッタ (time jitter) が導入されることがある。この実施例では、ストリーム内に全てのパケットを維持することによって、この問題を回避している。この実施例では、旧型のスクランブル装置は、パケットの再マッピングの処理、すなわちパケット P I D 「 A 」 から P I D 「 C 」 への再マッピング処理に参加しないため、旧型のスクランブル装置の製造業者による協力を必要としない。この再マッピングでは、旧型のスクランブル装置によって生成される P S I によって処理される P I D 「 C 」 を変更する必要がないという利点がある。旧型のシステムは、P I D 「 C 」 に関する知識を有するが、P I D 「 A 」 に関する知識は有さない。旧型のスクランブル装置によってスクランブルすべき全体的なエレメンタリストリームは、スクランブルシステムがスクランブルするように指示されている単一の P I D によって示される。

10

【0106】

上述の実施例において、第2の暗号化方式として用いる N D S は、例示的なものであり、本発明を限定するものではない。更に、広く用いられている2つの方式、すなわち、モトローラ社及びサイエンティフィックアトランタ社の方式を例示的に説明したが、他の旧型のシステムを同様に変更して P I D 再マッピング及びデュアル部分暗号化を実現することもできる。包括的には、上述した技術は、図13に包括的に示す処理800を含む。ステップ806においては、フィード (feed) を受信し、ステップ810において、このフィードをデスクランブルして、クリアなパケットのデータストリームを生成する。ステップ814において、所望のデュアル部分暗号化方式 (例えば、オーディオのみ、P E S ヘッダを含むパケット等) に応じてパケットを選択する。ステップ818において、選択されたパケットを複製し、複製された対を新たな2つの P I D (例えば、P I D 「 B 」 及び P I D 「 C 」) に再マッピングする。ステップ822において、複製されたパケットを P I D に基づいて暗号化する (すなわち、P I D 「 C 」 のパケットは、旧式の暗号化方式に基づいて暗号化し、P I D 「 B 」 のパケットは、新たな暗号化方式に基づいて暗号化する)。ステップ826において、クリアなパケットの P I D (例えば、P I D 「 A 」) を旧式の方式で暗号化されたパケットの P I D (P I D 「 C 」) と同じ P I D に再マッピングする。

20

30

【0107】

図13に示す処理800の各ステップの実行順序は、用いられるデュアル部分暗号化構成を含めるように変更される特定の旧型の方式に応じて、様々に変更してもよい。例えば、新たな暗号化方式に基づく暗号化は、複製を行う時点で行ってもよく、図11及び図12に示すように、後に旧式のパケットを再マッピングする際に、更に (図13には示さないが) 併用する特定の旧式の方式に対応するために、必要に応じて、様々な復調及び再変調処理を行ってもよい。

40

【0108】

セットトップボックスの実現

本発明の範囲内において、様々なセットトップボックスの構成を用いることができる。ヘッドエンドにおいて、暗号化するためのパケットを選択する手法は、S T B には無関係である。

【0109】

このような実現例の1つを図14に示す。この実施例では、チューナ及び復調器904からのパケットは、デコーダ回路908のデマルチプレクサ910に供給される。パケットは、(例えば、統合メモリアーキテクチャ (unified memory architecture) を用いて) メモリ912にバッファリングされ、R O M メモリ920に格納されているソフトウェ

50

アに基づいて動作する S T B のメイン C P U 9 1 6 によって処理される。

【 0 1 1 0 】

選択された P I D は、 S T B の P I D フィルタによって、供給されてくるトランスポートストリームから抽出され、 P V R アプリケーションにおける H D D への転送を準備するために必要な初期的な処理と同様に、復号され、 S D R A M にバッファリングされる。ホスト C P U 9 1 6 は、「非自動で (manually)」 S D R A M にバッファリングされたデータをフィルタリングし、不必要な P I D を含むパケットを除外する。この処理には、幾つかの明らかな副次的作用 (obvious side effects) がある。

【 0 1 1 1 】

ホスト C P U のオーバヘッドは、 C P U の帯域幅の約 1 % と推定される。最悪の場合、このオーバヘッドは、 1 5 M ビット / 秒のビデオストリームにおける 4 0 k バイト / 秒に相当する。評価されるデータは、各パケットについて多くても 4 バイトのみであり、これらは、 1 8 8 バイト分の間隔をあけて現れるので、間にあるデータは考慮しなくてもよく、このような削減が可能である。したがって、 S D R A M 内の各パケットヘッダは、メモリポインタの簡単な操作によって、直接読み出すことができる。更に、パケットは、ブロックにキャッシュされ、まとめて評価されるため、ホスト C P U の切替タスクを軽減することができる。

【 0 1 1 2 】

これにより、新たな各パケットを受け取る毎に、他のタスクに割込が生じることを回避することができる。このような処理では、チャンネルの変更時に、キャッシュを満たすために必要な時間分、デコードの開始のための待ち時間が長くなる。このような待ち時間は、割り当てられる S D R A M キャッシュのバッファサイズによっては、無視することができる程度のものである。

【 0 1 1 3 】

S D R A M バッファ内のホスト C P U でフィルタリングされパケットは、既存のハードウェア D M A 処理によって A / V キュー (A/V Queue) に転送され、 P V R の動作を模倣する。

【 0 1 1 4 】

セットトップボックスの第 2 の構成例を図 1 5 に示す。デコーダ I C 9 3 0 内の R I S C プロセッサ A / V デコーダモジュールは、パーシャルトランスポート P I D を処理し、デコードのための抽出及び結合を行うので、デコーダ I C 9 3 0 内のファームウェアは、各パケットヘッダ内の基準に基づいて、パーシャルトランスポートストリーム内の個々のパケットを除外することができる。これに代えて、デマルチプレクサ 9 1 0 によってパケットを除外するように設計してもよい。旧式の方式によってスクランブルされたパケットは、暗号化されたまま、 C A モジュールを通過する。デコーダ I C 9 3 0 を用いて、旧式の方式によってスクランブルされたパケットを取り除くことによって、及び新たな暗号化アルゴリズム (例えば、 N D S) によって暗号化されているパケットが旧式の方式で暗号化されたパケットに隣接して存在すると (又は、少なくとも次の第 1 のストリームビデオパケットより先に配置されていると) 仮定すると、旧式のパケットの除外により、事実上、単一のクリアなストリームがヘッダストリップ及びビデオキューにマージされることとなる。

【 0 1 1 5 】

セットトップボックスにおいて、部分暗号化を行うための第 3 の構成例を図 1 6 に示す。この実施例では、チューナ及び復調器 9 0 4 とデコーダ I C 9 0 8 との間に設けられた A S I C、フィールドプログラマブルゲートアレイ (Field Programmable Gate Array : F P G A)、プログラマブルロジックデバイス (programmable logic device : P L D) 9 3 8 又はこの他の専用に設計された回路によって P I D 再マッピングを行う。この実施例の変形例として、デコーダ I C 9 0 8 を変更し、 P I D 再マッピングをデマルチプレクサ 9 4 0 内で行うようにしてもよい。いずれの場合も、旧式の方式によって暗号化されたパケットは除外され、非旧式のパケットが回路 9 3 8 又はデマルチプレクサ 9 4 0 で再マ

10

20

30

40

50

ッピングされる。

【0116】

この第3の手法は、一実施例においては図17に示すPLDを用いて実現してもよい。この実施例では、特定のPIDを有する暗号化されたパケットは、連続して最大1個までしか現れないと仮定し、したがって（後述するように）、例えば、上述したM番目N暗号化構成とともに、暗号化されたパケットのバーストに対応するように構成を変更する。入力ストリームは、PIDに基づいて、入力ストリームを逆多重化するPID判別器950を通過する。連続カウンタ確認器958は、第1のPIDパケットの連続性を確認する。連続性にエラーが検出された場合、ブロック960において、このエラーが検出され、カウンタがリセットされる。

10

【0117】

元の入力パケットストリームは、多数のPIDによってタグが付されたパケットを含む。PID判別器950は、所定の2つのPID（第1及び第2のPID）を有するパケットを他の全てのパケットから分離する。この機能は、複数の対を処理するように拡張してもよい。これらの他のパケットは、変更された（revised）出力ストリームに直接バイパスされる。この処理では、3バイト又は4バイトのクロック遅延が生じる。

【0118】

第2のPIDを有するパケットは、PID判別器950によって、連続カウンタ確認器954にルーティングされ、連続カウンタ確認器594は、このPIDについて、シーケンスの完全性を検証する。ブロック956は、エラーを検出するが、このエラーの処理は、本発明に直接関係しないため詳細には説明しない。パケットの連続性を示す値は、後のパケットのシーケンスの確認に使用するために保存される。連続カウンタ確認器958は、独立した第1のカウンタを用いて、第1のPIDを有するパケットについて、対応する連続性を確認し、ここでも、ブロック960においてエラーが検出される。

20

【0119】

ブロック962において、第2のパケットに第2のフラグがあるか否かが判定される。このブールインジケータ（Boolean indicator）は、直前のクリアなパケット以来、第2のパケットが処理されていることを記憶するために用いられる。この実施例では、クリアなパケット間に2つ以上の第2のパケットがあるとエラーとなり、ブロック964において、このエラーが検出される。第2のパケットの存在は、ブロック966において、第2のフラグを設定することによって以後の処理に示される。

30

【0120】

第2のパケットの連続カウンタは、ブロック968において、クリアなパケットのシーケンスに適合するように変更される。ブロック958において、この置換（substitution）のためのデータは、連続カウンタ確認器958において第1のストリームの連続性を検証するために用いた値に由来する。変更されたパケットは、ブロック968から出力され、変更されたストリームにマージされ、これにより出力ストリームが生成される。

【0121】

第1のPIDを有するパケットが連続カウンタ確認器958において、連続性を確認された後、これらのパケットは、ブロック970において、ヘッダ内のスクランブルフラグ（scrambling flag）によって区別される。パケットがスクランブルされている場合、ブロック974において、第1のフラグが要求される。この第1のフラグであるブールインジケータは、直前のクリアなパケット以来、第1のパケットが処理されていることを記憶するために用いられる。この実施例では、クリアなパケット間に2つ以上の第1のパケットがあるとエラーとなり、ブロック976において、このエラーが検出された後、ブロック978においてパケットが削除される。第1のパケットの存在は、ブロック978において、第1のフラグを設定することによって以後の処理に示される。暗号化されたパケットを使用するユーザがダウンストリーム側にいない場合、ブロック978において、このパケットを削除してもよい。幾つかの状況では、このパケットを継続する必要がある場合がある（この場合、その連続カウンタは、除外して第2の継続値を用いることができる）

40

50

。

【 0 1 2 2 】

ブロック 9 7 0 における第 1 の P I D のスクランブル検査によって、クリアなパケットが検出された場合、ブロック 9 8 4 において、第 2 及び第 1 のフラグの状態が検査される。暗号化されたパケットは、常に対として存在するため、有効となる条件は、この対の両方が存在しない場合か、両方が存在する場合のいずれかである。これらの対のうち的一方のみが存在する状況は、ブロック 9 8 8 においてエラーと判定される。但し、この実施例では、出現の順序は問題としない。なお、第 1 のパケットに削除のためのフラグを付す手法としては、例えばトランスポートプライオリティビット (TRANSPORT_PRIORITY) 等のトランスポートヘッダのビットをスクランブルしてもよく、これ以外の手法を用いてもよい。更に、如何なるビットも使用せず、例えば、第 1 (第 2) のパケットが第 2 (第 1) のパケットの前にあるか後にあるかといった第 1 (第 2) のパケットの単純な位置情報をインジケータとして用いてもよい。

10

【 0 1 2 3 】

第 1 の P I D を有するクリアなパケットの P I D 値は、ブロック 9 9 2 において、第 2 の P I D に変更された後、変更された出力ストリームに組み込まれる。これに代えて、第 2 の P I D を有するパケットを第 1 の P I D 値に再マッピングしてもよい。コンテンツをデコードするための正しい P I D (第 1 の又は第 2 の P I D のいずれか) がデコーダに供給されると、コンテンツをデコードすることができる。クリアなパケットの存在は、第 1 又は第 2 のブールフラグによって示される。

20

【 0 1 2 4 】

上述した全ての実施例において、一連の第 1 のパケットに置換のためのタグが付されていても、第 2 のパケットを置換すべき第 1 のパケットに隣り合うように挿入することができる。なお、幾つかの実施例では、第 2 のパケットを介在させることなく、複数の暗号化されたパケットをストリームに挿入できる場合、ヘッドエンド部分スクランブルを行ってもよい。(例えば、M 番目 N 部分暗号化方式のように) 複数の連続する暗号化されたパケットをストリームに含ませるために、第 1 及び第 2 のフラグの使用を、カウンター一致検査機能 (counter matching test function) に置き換えてもよい。この場合、ブロック 9 6 2、9 6 4、9 6 6 に代えて、第 2 の暗号化パケットカウンタをインクリメントする。また、ブロック 9 7 0、9 7 4、9 7 6、9 8 0 に代えて、第 1 の暗号化パケットカウンタをインクリメントする。ブロック 9 8 4 は、第 1 及び第 2 のパスから、同じ数の暗号化されたパケットが受け取られていることを確認するための第 1 及び第 2 の暗号化パケットカウンタの比較に置き換えられる。また、ブロック 9 9 2 においてフラグを消去するのに代えて、ここでは、カウンタをリセットするこの変形例により、複数の暗号化されたパケットを継続的に受け取ることができ、受け取られたパケットの数を比較して、データストリームの完全性を監視することができる。当業者は、この他の変形例を想到することもできる。

30

【 0 1 2 5 】

図 1 7 を用いて上述した機能は、市販されているセットトップボックスにおいて使用されており、市場から入手することができるブロードコム (Broadcom) シリーズ 7 0 x x 又は 7 1 x x デコーダの機能と同等の機能を有する A / V デコーダチップに統合してもよい。図 1 8 は、このようなデコーダチップのブロック図であり、ここでは、市販されているチップにおいて既に設けられている機能は、基本的に変更していない。通常、市販されているデコーダチップは、P I D と番組コンポーネント (例えば、オーディオ、ビデオ) との間に対一の対応関係があることを前提に設計されている。

40

【 0 1 2 6 】

図 1 8 に示すデコーダは、メインオーディオと、メインビデオと、ピクチャインピクチャ (picture-in-picture: P i P) 機能に用いるセカンダリビデオとについて、第 1 及び第 2 の P I D を処理できるように、S T B の C P U への接続を介して、複数の P I D がデコーダにプログラミングされることを許容するこの実施例では、生のデータストリームが

50

図17を用いて上述した、PIDに基づいてパケットのストリームを逆多重化する機能と同様の機能を有するパケットソータ1002によって受け取られる。好ましくは、図18に示すデコーダは、プログラミングされたソフトウェアではなく、ハードワイヤード論理回路を用いて、パケットソータ1002におけるPIDソート機能を実現する。番組ガイド及びストリームナビゲーション情報は、例えば、STBのCPUによって使用するために出力される。メインオーディオ番組に関連するパケットは、FIFO1006内にバッファリングされた後、復号器1010によって復号され、バッファ1014にバッファリングされ、MPEGオーディオデコーダ1018によって、必要なときに読み出される。デコードされたMPEGオーディオ信号は、デコーダからの出力信号として出力される。

【0127】

同様に、メインビデオ番組に関連するパケットは、FIFO1024内にバッファリングされた後、復号器1028によって復号され、バッファ1032にバッファリングされ、MPEGビデオデコーダ1036によって、必要なときに読み出される。メインチャンネルのデコードされたMPEGビデオ信号は、後述する混合器(composer)1040に供給され、ここから、デコーダからの出力信号として出力される。同様に、ピクチャインピクチャビデオに関連するパケットは、FIFO1044内にバッファリングされた後、復号器1048によって復号され、バッファ1052にバッファリングされ、MPEGビデオデコーダ1056によって、必要なときに読み出される。ピクチャインピクチャチャンネルのデコードされたMPEGビデオ信号は、混合器1040に供給され、ここで、メインチャンネルビデオ信号と合成され、ここから、デコーダからの出力信号として出力される。メインチャンネル又はピクチャインピクチャチャンネルに関連しない他のパケットは削除される。勿論、本発明の範囲から逸脱することなく、他の機能をデコーダチップに組み込み、又はデコーダチップから既存の機能を削除してもよい。

【0128】

結論

上述のように、ハッカーからの執拗な攻撃に対抗するために、上述した部分暗号化構成の幾つかを組み合わせ、更に安全性を高めてもよい。例えば、クリティカルパケット暗号化は、安全性を高めるために、SI暗号化、M番目N暗号化、ランダム暗号化、タイムスライス暗号化、及び他の手法のいずれと組み合わせてもよい。一実施例においては、帯域幅が許す限り、可能な限り多くのパケットを暗号化する。暗号化の量は、コンテンツがレギュラー番組であるか、プレミア番組(例えば、ペイパービュー又はVOD)であるか、コンテンツがアダルト番組であるか通常の映画であるか、或いは、様々なケーブルオペレータが適当と認める安全性のレベルに応じて決定してもよい。本発明の範囲から逸脱することなく、暗号化の安全性を更に高めるために他の様々な組合せが可能であることは、当業者にとって明らかである。

【0129】

上述した様々な実施例では、MPEG2符号化を用いたデジタルA/Vシステムに関連して本発明を説明した。したがって、様々なパケット名及びプロトコルとしては、MPEG2符号化及び復号に関連するものを用いた。しかしながら、ここに開示し、特許を請求する概念は、このような範囲に限定されるものではないことは当業者にとって明らかである。同様の又は類似する手法は、MPEG2プロトコルに限定されることなく、如何なるデジタルケーブルシステムにおいても実現できる。更に、本発明の手法は、例えば、以下に限定されるものではないが、地上波放送を用いたコンテンツ配信方式、インターネットを用いたコンテンツ配信方式、例えば、DirecTV(商標)等で用いられているデジタル衛星サービス(Digital Satellite Service: DSS)等の衛星を用いたコンテンツ配信方式、及びパッケージ媒体(例えば、CDやDVD)を含む他の適切な如何なるコンテンツ配信シナリオにおいて実現してもよい。これらに基づく様々な変形例は、ここに説明した技術と等価であり、ここに例示的に説明したMPEG2ケーブルシステムの実施例は、本発明を例示的に説明するための一具体例と解釈するべきである。

【0130】

10

20

30

40

50

更に、テレビジョンセットトップボックスを用いて、部分的に暗号化されたテレビジョン番組を復号する具体例によって本発明を説明した。しかしながら、本発明に基づく復号メカニズムは、STBを備えないテレビジョン受信機においても同様に実現でき、更に、MP3プレイヤー等のミュージックプレイヤーにおいても実現できる。これらの実施例も、ここに説明した実施例と等価である。

【0131】

更に、テレビジョン番組のデュアル部分暗号化のためのメカニズムを提供するための暗号化方式に関連して本発明を説明したが、部分暗号化方式は、単一の暗号化方式、又は2つ以上の暗号化方式における複数の暗号化方式としても制限なく用いることができる。暗号化された更なる複製されたパケットに2つ以上の暗号化方式を適用してもよい。また、複製されたパケットの1つのための暗号化鍵を複数の暗号化方式間で共有してもよい。更に、ここでは、特にテレビジョン番組の暗号化を行う特別な目的について説明したが、本発明は、以下に限定されるものではないが、インターネット又は他のネットワークからダウンロードされるコンテンツ、音楽コンテンツ、パッケージ媒体、及びこれらの他の種類の情報コンテンツを含む他のコンテンツを単独で暗号化し又はデュアル部分暗号化するために用いてもよい。更に、本発明の範囲から逸脱することなく、これらのコンテンツは、以下に限定されるものではないが、例えば、携帯情報端末(personal digital assistant: PDA)、パーソナルコンピュータ、個人用ミュージックプレイヤー、オーディオシステム、オーディオ/ビデオシステム等を含む如何なる再生機器において再生してもよい。

10

【0132】

当業者には明らかであるが、ここでは、プログラミングされたプロセッサを用いて実現できる例示的な実施例を用いて本発明を説明した。しかしながら、本発明は、このような実施例に限定されるわけではなく、本発明は、特定用途のハードウェア等のハードウェアコンポーネントの等価物を用いても実現でき、及び/又は専用のプロセッサを用いても実現でき、このような実現例は、ここに開示し、請求の範囲において請求する本発明と等価である。同様に、汎用コンピュータ、マイクロプロセッサを用いたコンピュータ、マイクロコントローラ、光コンピュータ、アナログコンピュータ、専用プロセッサ、及び/又は専用ハードワイヤード論理回路を用いて、本発明の実施例と等価な構成を構築することもできる。

20

【0133】

また、上述の実施例を実現するためのプログラミングのステップ及びこれらに関連するデータは、本発明の範囲を逸脱することなく、読出専用メモリ(Read Only Memory: ROM)素子、ランダムアクセスメモリ(Random Access Memory: RAM)素子、光ストレージ装置、磁気ストレージ装置、光磁気ストレージ装置、フラッシュメモリ、コアメモリ、及び/又はこの他の同等のストレージ技術を用いても実現できる。これらと同様のストレージ装置は、等価物とみなすことができる。

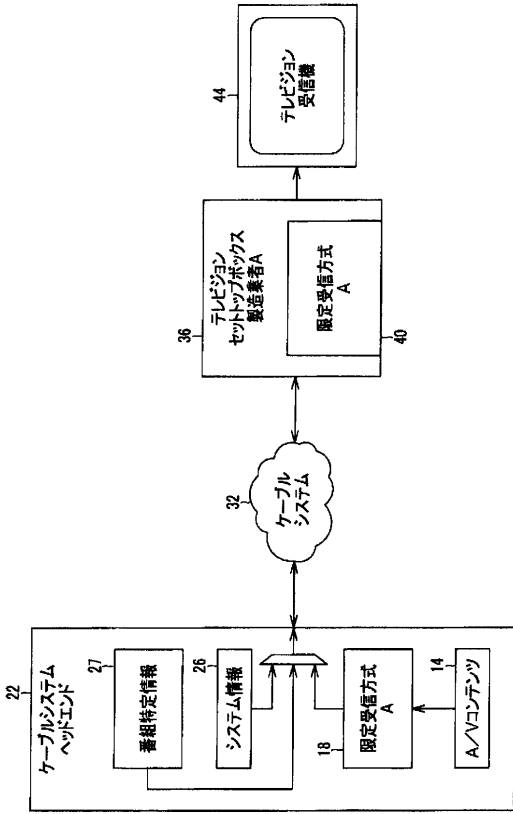
30

【0134】

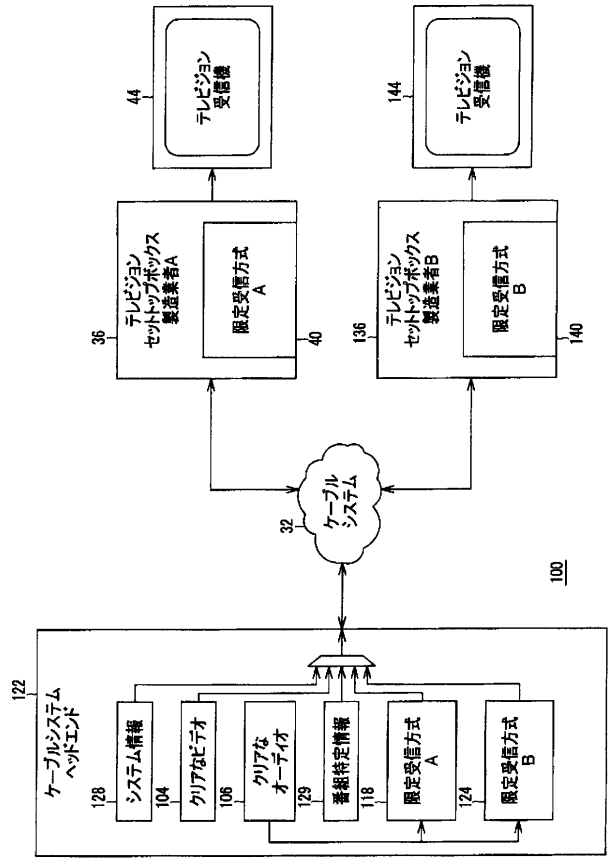
本発明は、先にフローチャートを用いて広く説明し、適切な電子ストレージ媒体に格納でき、又は適切な電子通信媒体を介して伝送できるプログラミング命令を実行するプログラミングされたプロセッサを用いて実現することができる。なお、上述した処理は、本発明の範囲を逸脱することなく様々に変形でき、様々な適切なプログラミング言語を用いて記述できることは当業者にとって明らかである。例えば、本発明の範囲から逸脱することなく、実行される動作の順序を変更でき、他の動作を加えることも幾つかの動作を省略することもできる。また、本発明の範囲を逸脱することなく、エラー修正処理を追加及び/又は拡張してもよく、ユーザインタフェース及び表示される情報を様々に変更してもよい。これらの変形も等価であるとみなされる。

40

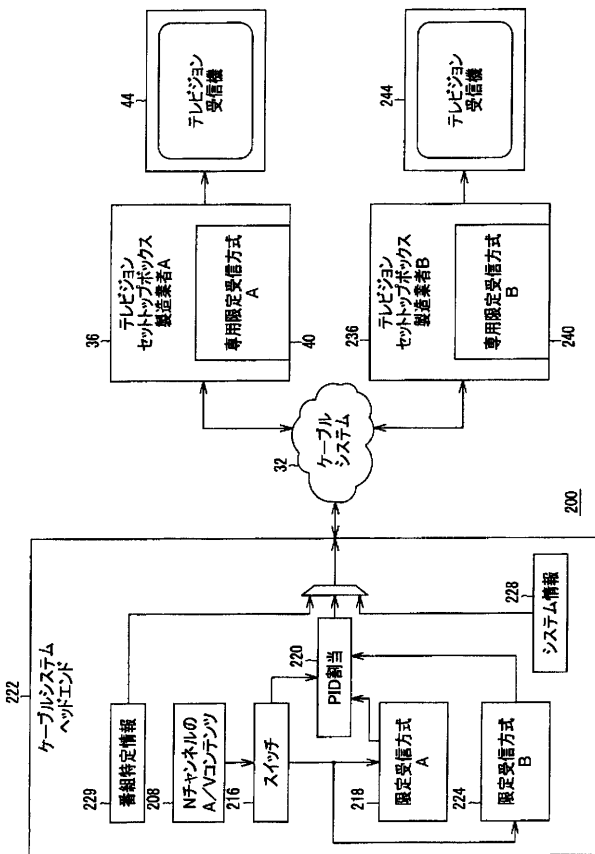
【図1】



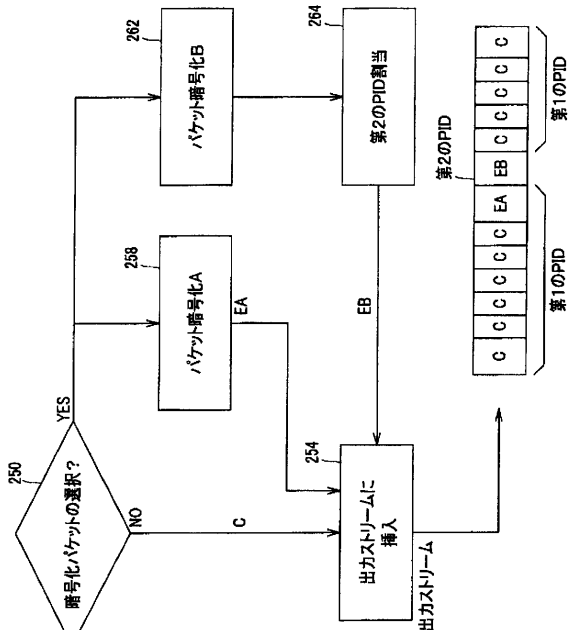
【図2】



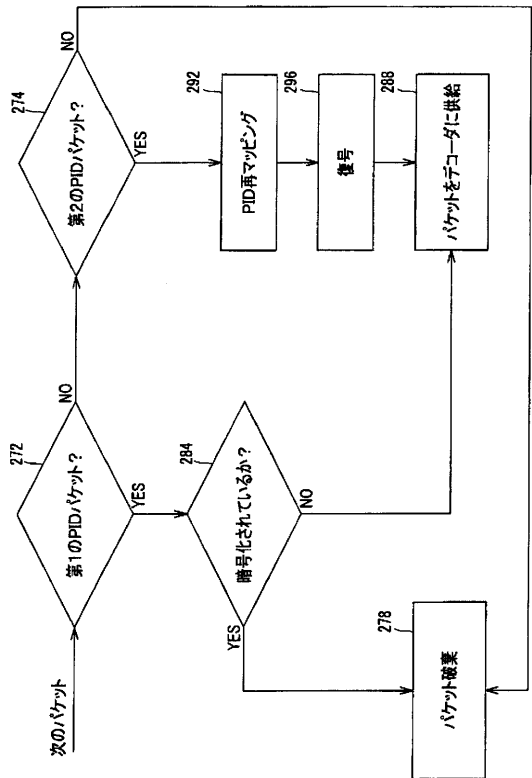
【図3】



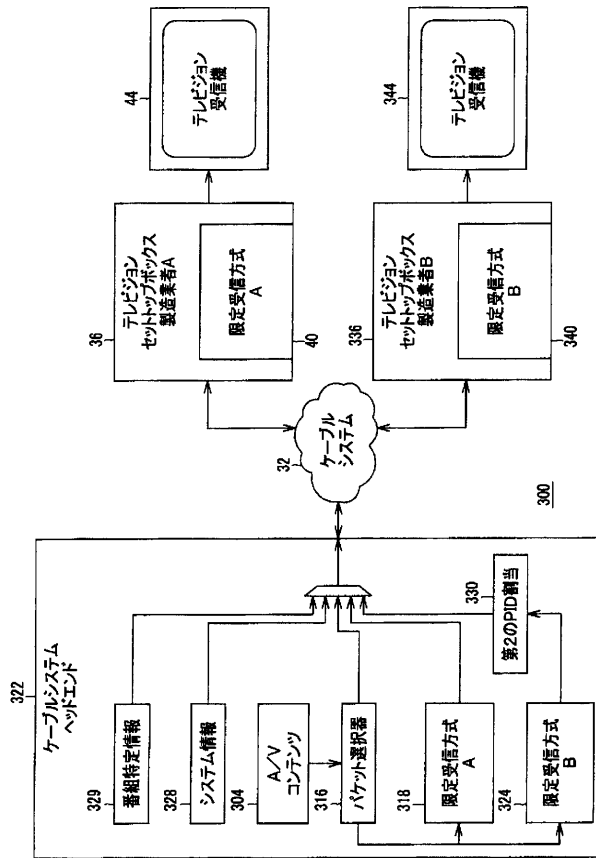
【図4】



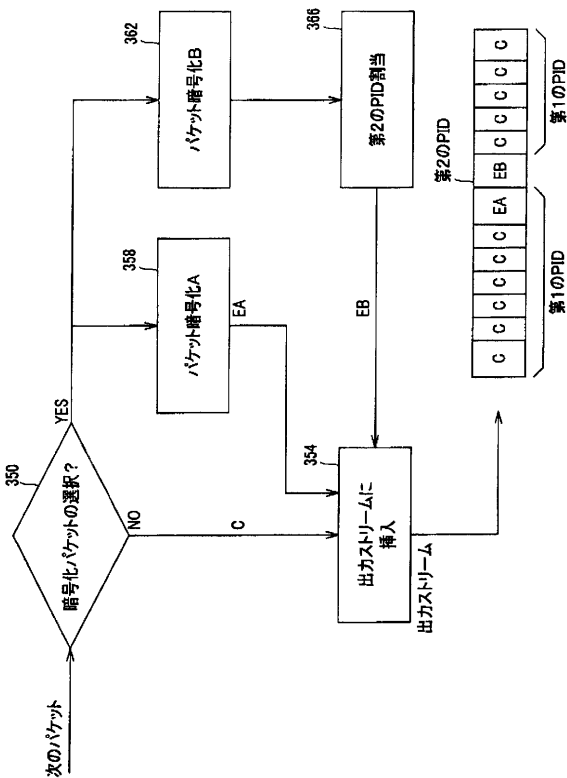
【 図 5 】



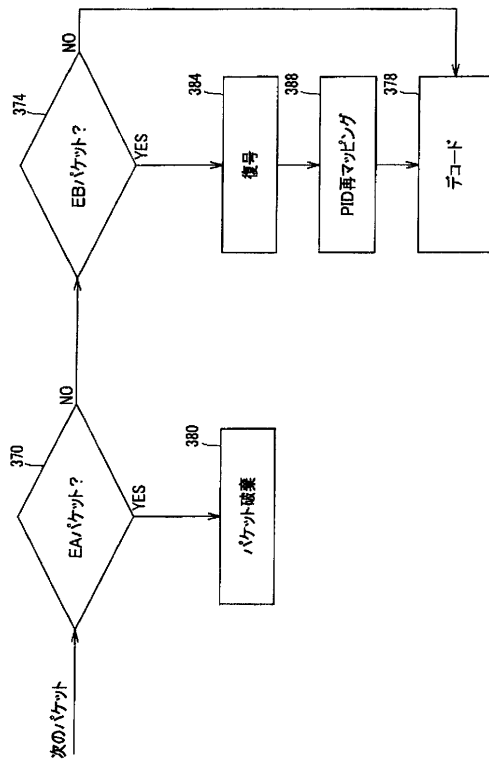
【 図 6 】



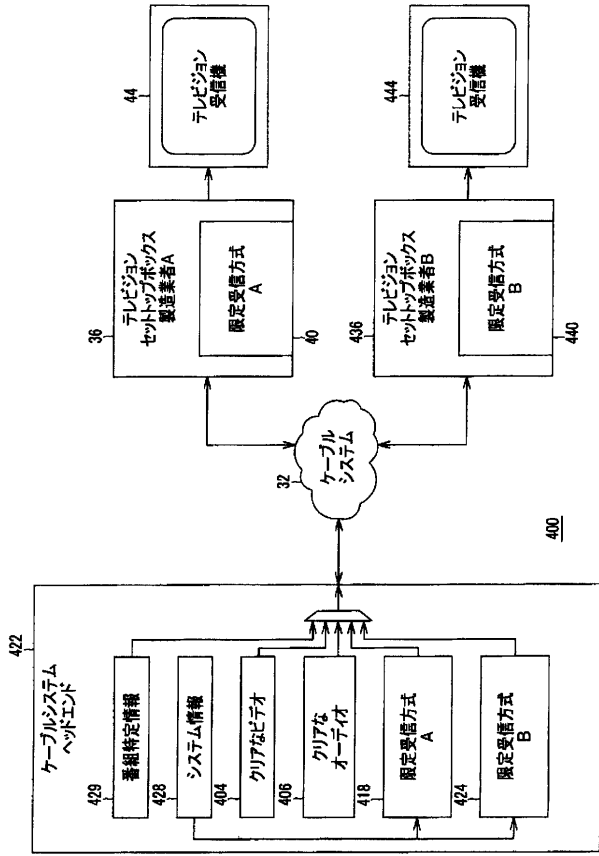
【 図 7 】



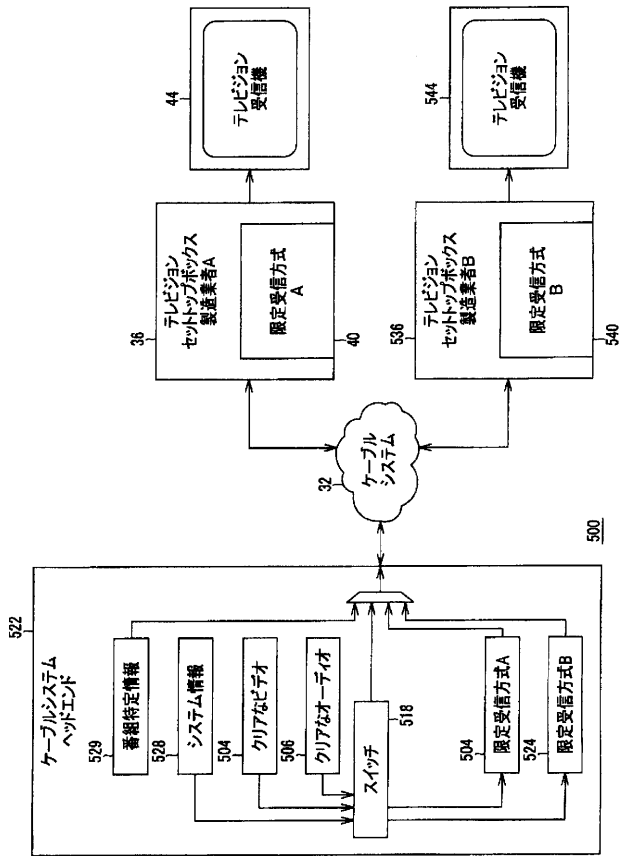
【 図 8 】



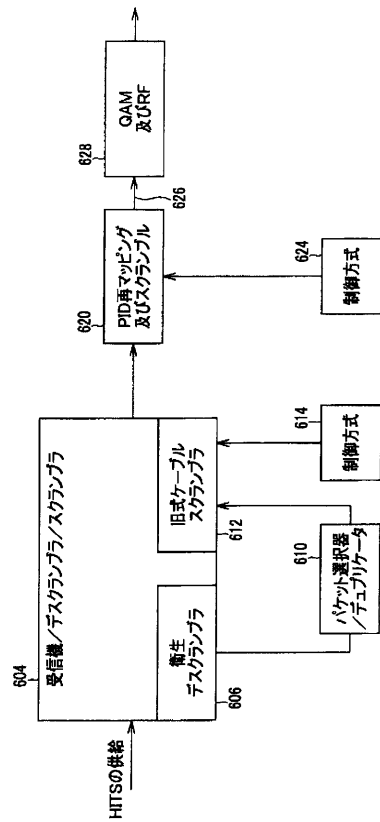
【 図 9 】



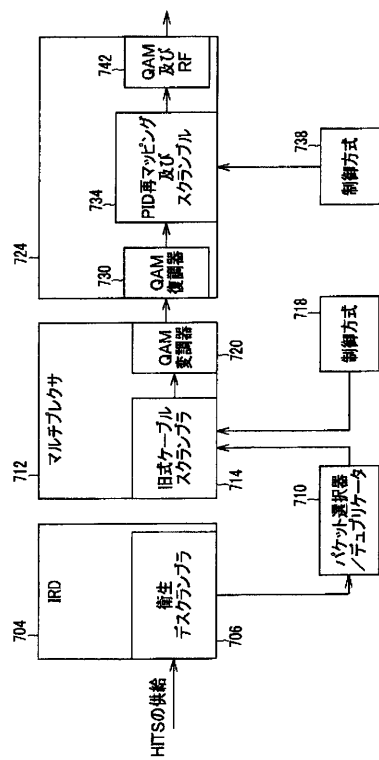
【 図 10 】



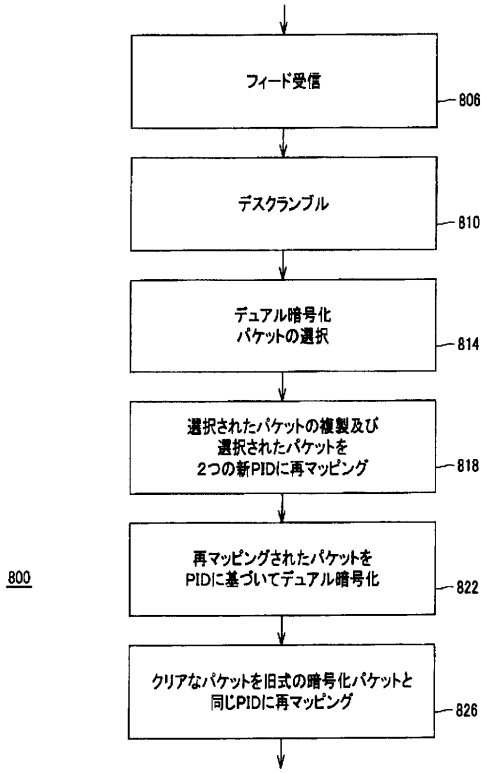
【 図 11 】



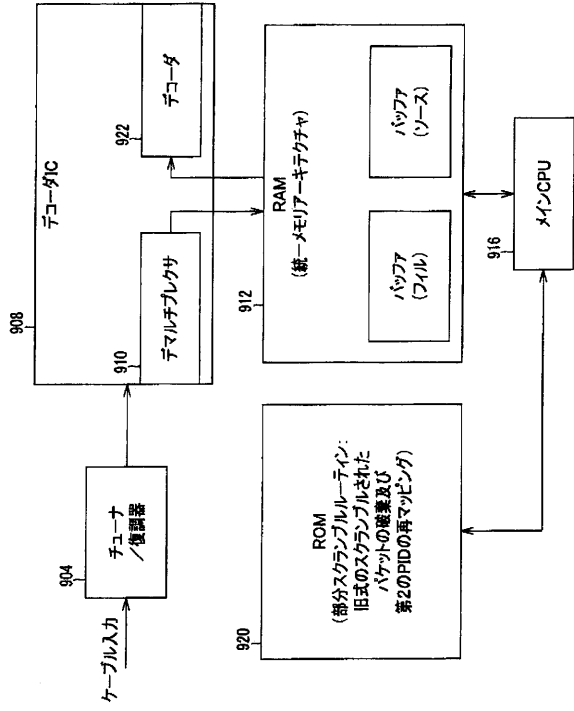
【 図 12 】



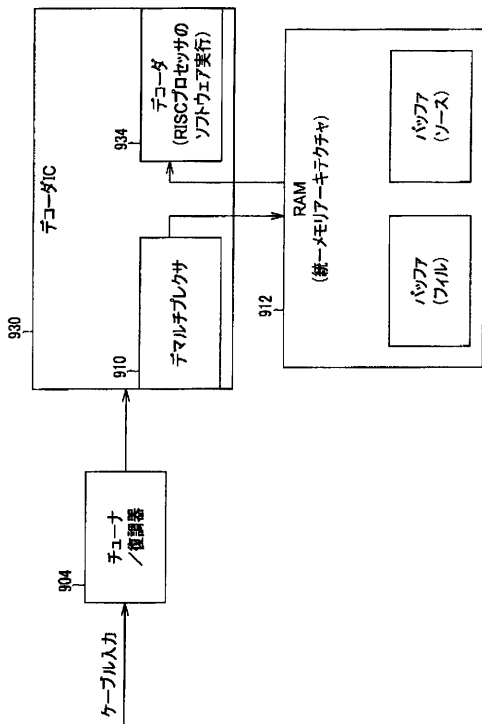
【 図 1 3 】



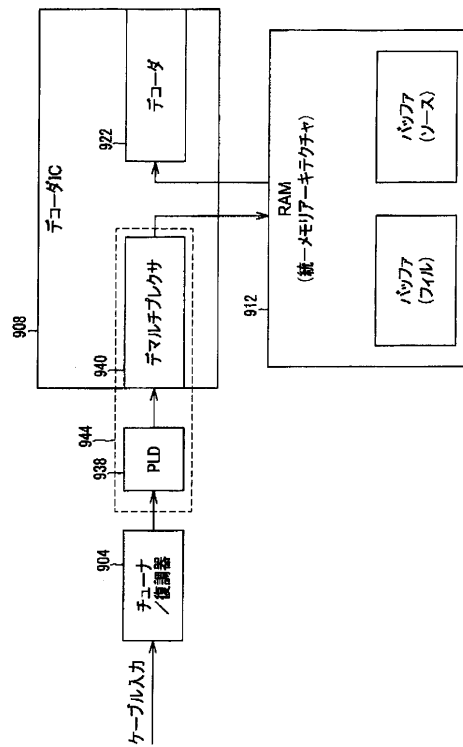
【 図 1 4 】



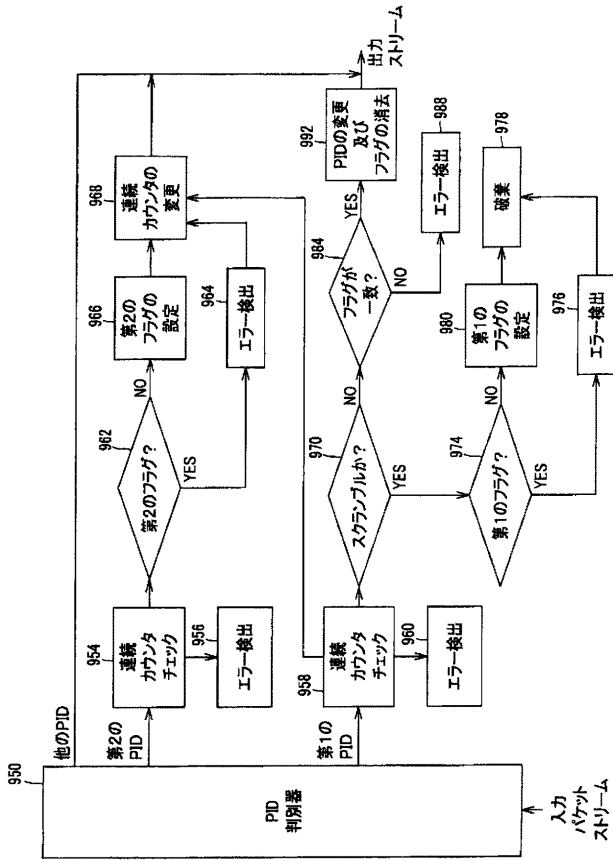
【 図 1 5 】



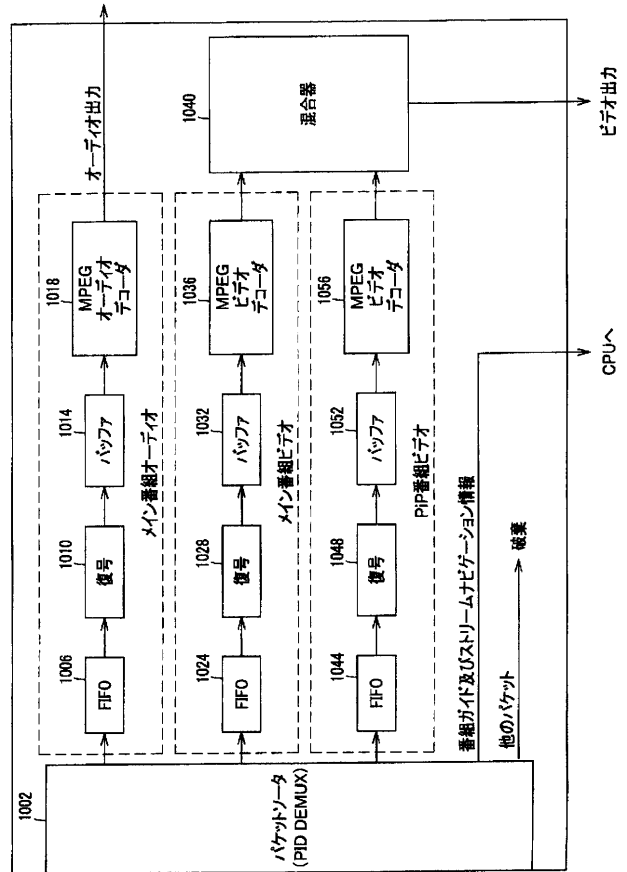
【 図 1 6 】



【 図 1 7 】



【 図 1 8 】



【 手続補正書 】

【 提出日 】 平成21年12月9日 (2009.12.9)

【 手続補正 1 】

【 補正対象書類名 】 明細書

【 補正対象項目名 】 全文

【 補正方法 】 変更

【 補正の内容 】

【 発明の詳細な説明 】

【 技術分野 】

【 0 0 0 1 】

本発明は、暗号化システムに関し、より詳しくは、デジタルテレビジョン信号の部分的な暗号化及び復号を行うシステム、方法及び装置に関する。

【 0 0 0 2 】

[関連出願]

本出願は、2001年6月6日に提出されたカンデロア他の米国仮出願番号第60/296,673号「あるコンテンツのビデオをクリアに、及び他のコンテンツのビデオ及びオーディオのデュアルキャリッジを送信することによって、複数のCAプロバイダがコンテンツ配信システムにおいて相互運用を行うことができる方法 (Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Sending Video in the Clear for Some Content, and Dual Carriage of Audio and Dual Carriage of Video and Audio for Other Content)」、2001年7月10日に提出されたアンガー他の米国仮出願番号第60/304,241号「デュアルキャリッジのプログラムコンテンツの自由に選択可能な暗号 (Independent Selective Encryptions of Program Content for Dual Carriage)」、2001年7月10日に提出されたカンデロア他の米国仮出願番号第60/304,131号「タイムスライス方式においてコンテンツに部分的にスク

ランブルを掛けることによって、複数のCAプロバイダが相互運用を行うことができる方法 (Method for Allowing Multiple CA Providers to Interoperate in a Content Delivery System by Partial Scrambling Content on a Time Slice Basis) 」及び2001年10月26日に出願されたカンデロア他の米国仮出願第60/343,710号、代理人整理番号SNY-R4646P「テレビジョン暗号化システム (Television Encryption System) 」に関連し、これら関連出願は、参照により本願に援用される。

【0003】

本出願は、アンガー他の米国特許出願第10/038,217号、代理人整理番号SNY-R4646.01「重要なパケットの部分的な暗号化 (Critical packet Partial Encryption) 」、カンデロア他の米国特許出願代理人整理番号SNY-R4646.02「時間分割の部分的な暗号化 (Time Division Partial Encryption) 」、アンガー他の米国特許出願第10/037,914号、代理人整理番号SNY1-R4646.03「エレメンタリストリーム部分暗号化 (Elementary Stream Partial Encryption) 」、及びアンガー他の米国特許出願第10/037,498号代理人整理番号SNY-R4646.05「部分的に暗号化された情報の復号及び解読 (Decoding and Decrypting of Partially Encrypted Information) 」と同時に提出されている。これらの同時に出願された米国出願は、参照により本願に援用される。

【0004】

[著作権表示]

この明細書の開示内容の一部は、著作権保護の対象となる資料を含んでいる。著作権者は、この明細書が特許商標庁への特許出願又は記録であると認められるファックスコピー又は特許開示に対しては異議を唱えないが、それ以外のあらゆる全ての著作権を保有する。

【背景技術】

【0005】

テレビジョンシステムは、視聴者に娯楽番組及び教育番組を配信するために用いられる。ソースマテリアル (オーディオデータ、ビデオデータ等) は、混合信号 (combined signal) に多重化され、この混合信号は搬送波を変調するために用いられる。この搬送波は、一般に、チャンネルとして知られている (典型的なチャンネルでは、1つのアナログ番組、1つ又は2つの高精細度 (HD) デジタル番組、又は複数の (例えば9つの) 標準解像度のデジタル番組を送ることができる)。地上波システムにおいて、これらのチャンネルは、行政割当の周波数 (government assigned frequencies) に対応し、電波によって放送される。番組は、受信機に配信され、受信機はチューナを備え、チューナは、電波から信号を検波して、復調器に供給し、復調器は、映像をディスプレイに、音声をスピーカから出力する。ケーブルシステムにおいては、変調チャンネルは、ケーブルを介して送られる。また、視聴可能な番組及び関連した選局情報を示す番組ガイドを、チャンネルの帯域内又は帯域外で提供することもできる。ケーブルシステムではチャンネルの数は、限られており、すなわち機器及びケーブルの帯域幅によって制限される。ケーブルの敷設 (CABLE distribution systems) には、巨額の設備投資がかかり、その改良にも費用がかかる。

【0006】

テレビジョンコンテンツの多くは、その製作者にとって貴重なものであり、したがって、著作権者は、アクセスを制御し、コピーを制限することを望んでいる。典型的な著作権保護のマテリアル (protected material) の例としては、長編映画 (feature film)、スポーツ競技の番組、成人番組がある。限定受信 (conditional access: 以下CAという。) 方式は、ケーブルシステム等のコンテンツ配信システムにおける番組の視聴 (availability) を制御するために用いられる。CA方式は、ケーブルシステムのヘッドエンドに組み込まれ、有料コンテンツ (premium content) を暗号化する部分と、ユーザの家庭に設置されたセットトップボックス (set-top box: 以下STBという。) に内蔵され、復号を行う部分との組合せ (matched set) として提供される。ケーブルテレビ業界では、N

D S 社（米国カリフォルニア州ニューポートビーチ）、モトローラ社（米国イリノイ州シウンバーグ）、サイエンティフィックアトランタ社（米国ジョージア州アトランタ）によって提供されている C A 方式を含む幾つかの C A 方式が使用されている。C A 方式における暗号化部と復号部を整合させなければならないという状況により、「旧型（"legacy"）」の S T B の製造業者は、この S T B を供給し続けなければならない。限定受信の様々な技術は、互換性がない（且つ、多くの場合、独占（proprietary）されている）ので、新規に参入する供給業者は、旧式の C A 方式のライセンスを受けることを余儀なくされる。したがって、C A 方式技術の保有者は、多くの場合、協力又は適正な実施料を請求する気がなく、ケーブルテレビの運用業者は、他のセットトップボックス製造業者からより新しい技術又は競合する技術を取得することができない。このように技術的互換性がないために、異なる C A 方式を採用しているケーブルテレビ会社が合併する際には、特に問題がある。サービス提供業者は、数多くの理由から、S T B 供給元が複数あることを希望する。

【 0 0 0 7 】

ケーブルテレビ運用業者は、一旦、あるコンテンツ暗号化方式（encryption scheme）を採用すると、下位互換性のある復号装置（例えばセットトップボックス）を導入することなく、そのコンテンツ暗号化方式を変更又は更新することは困難になる。S T B の製造業者は、複数の復号機能を提供する技術があっても、新しいセットトップボックスに複数の暗号化方式に対応するようなマルチモード機能を付けると、この新しいセットトップボックスにはかなりの原価がかかってしまう。

【 0 0 0 8 】

旧型の S T B の製造業者による支配を避けるための現在知られている唯一の選択肢は、（大規模な交換を除いて）「フルデュアルキャリッジ（full dual carriage）」を用いることである。フルデュアルキャリッジとは、それぞれの暗号化された番組に対して、用いられている C A 暗号化の種類毎に、二重に伝送することを意味する。フルデュアルキャリッジを提供するためには、ヘッドエンドを、各 C A 方式を同時に提供するように増強しなければならない。如何なる変更があった場合でも、旧型の S T B は、影響を受けず、その機能を実行し続けなければならない。しかしながら、フルデュアルキャリッジでは、多くの場合、帯域が重なることを避けるためには視聴可能な番組の数を減らさなければならず、受け入れ難い料金となっている。通常、有料チャンネルの数が少なくなると、視聴者の視聴可能な選択肢も限定され、ケーブルテレビ運用業者が提供できる価値も制限される。

【 0 0 0 9 】

図 1 は、従来のケーブルシステムの構成を示すブロックである。このケーブルシステムでは、ケーブルテレビ運用業者は、ケーブルシステムヘッドエンド 2 2 において方式 A に準拠した C A 暗号化装置 1 8 を使い、製造業者 A（方式 A）の C A 技術によってオーディオ/ビデオ（A/V）コンテンツ 1 4 を処理する。暗号化された A/V コンテンツは、システム情報（system information：以下 S I という。）2 6 及び番組特定情報（program specific information：以下 P S I という。）2 7 が多重化され、ケーブルシステム 3 2 を介してユーザの S T B 3 6 に伝送される。S T B 3 6 には、暗号化された A/V コンテンツを復号する C A 方式 A（製造業者 A）の C A 復号装置が組み込まれている。復号された A/V コンテンツは、テレビジョン受信機 4 4 に供給され、ユーザによって視聴される。

【 0 0 1 0 】

図 1 に示すようなケーブルシステムにおいて、デジタル番組ストリームはパケットに分割されて伝送される。番組の各コンポーネント（ビデオデータ、オーディオデータ、補助データ等）のパケットには、パケット識別子（packet identifier：以下 P I D という。）が付加される。チャンネル内で送られる全ての番組の各コンポーネントに対するこれらのパケットストリームは、1つの複合ストリームに結合される。複合ストリームは、復号鍵及び他のオーバーヘッド情報を有する追加的なパケットも含んでいる。追加的なパケットがない場合、未使用の帯域は空パケットによって埋められる。帯域配分は、通常、利用可

能なチャンネル帯域幅の約95%を使用するように調整されている。

【0011】

オーバーヘッド情報は、通常、視聴可能な番組と、その関連するチャンネル及びコンポーネントの位置を特定する方法を示すガイドデータを含んでいる。このガイドデータは、システム情報、すなわちSIとしても知られている。SIは、STBに帯域内で(チャンネル内の暗号化データの一部として)又は帯域外で(この目的専用に設けられた特別のチャンネルを用いて)配信することができる。電子的に配信されるSIは、従来の種類の、すなわち新聞及び雑誌に記載された番組表を部分的に複製したものでよい。

【0012】

視聴者が満足の得られるテレビジョンの視聴をするためには、一般的に、暗号化されていない状態で(clear)オーディオコンテンツ及びビデオコンテンツの両方にアクセスできることが望ましい。幾つかのアナログケーブルシステムでは、料金を払っていない未許可の視聴者が番組を受信できないように、様々なフィルタリング技術を用いてビデオコンテンツを見えなくしている。このようなアナログケーブルシステムにおいては、アナログオーディオコンテンツは、鮮明(clear)に送られることもある。Cバンド衛星通信に用いられるモトローラ社のビデオサイファ2プラス(VideoCipher 2 Plus、商標)方式では、強力なデジタルオーディオ暗号化と、アナログビデオデータの比較的弱い(同期反転を用いた)保護との組合せが用いられている。航空会社の機内映画システムでは、料金を払ってヘッドホンを借りた乗客のみが、オーディオとビデオを完全に視聴できるという方法を用いている。

【発明の概要】

【課題を解決するための手段】

【0013】

本発明に係るコンテンツを暗号化する暗号化方法において、コンテンツの100%未満を暗号化する選択アルゴリズムに基づいて暗号化するコンテンツの部分特定し、特定されたコンテンツの部分特定を第1の暗号化方式に基づいて暗号化して、第1の暗号化された部分を生成し、特定されたコンテンツの部分特定を第2の暗号化方式に基づいて暗号化して、第2の暗号化された部分を生成し、暗号化されていない部分とともに、第1の暗号化された部分と、第2の暗号化された部分とを結合して、部分多重暗号化コンテンツを生成する。

【0014】

本発明に係るパケット化されたデジタルテレビジョン信号を符号化する符号化方法において、第1の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含むパケットの一部を暗号化し、第2の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含むパケットの一部を暗号化し、デジタルテレビジョン信号を含むパケットの一部を暗号化せずにそのまま残し、暗号化されていないパケットに第1のパケット識別子を割り当て、第1の暗号化アルゴリズムに基づいて暗号化されたパケットに第1のパケット識別子を割り当て、

第2の暗号化アルゴリズムに基づいて暗号化されたパケットに第2のパケット識別子を割り当てる。

【0015】

本発明に係るパケット選択及び複製装置は、衛星信号デスクランブラからクリアなパケットのストリームを受信する入力手段と、多重暗号化するパケットのグループを選択するとともに、クリアなパケットの組を残す選択手段と、選択されたパケットを複製し、第1及び第2の複製されたパケットの組を生成する複製手段と、第1のパケット識別子を第1の複製されたパケットの組に割り当て、第2のパケット識別子を第2の複製されたパケットの組に割り当てる割り当て手段と、第1の複製されたパケットの組と、第2の複製されたパケットの組と、クリアなパケットの組とを多重化してパケットの出力ストリームを生成する多重化手段とを備える。

【0016】

本発明に係るパケット識別子再マッピング装置は、第1のパケット識別子を有するクリ

アなパケットと、第2のパケット識別子を有する暗号化されたパケットと、第3のパケット識別子を有する暗号化されたパケットとからなる変調パケットのストリームを復調する復調器と、第1のパケット識別子を有するクリアなパケットと、第2のパケット識別子を有する暗号化されたパケットとが同じパケット識別子を有するようにパケット識別子を変更する再マッピング器とを備える。

【図面の簡単な説明】

【0017】

【図1】従来の限定受信ケーブルシステムの構成を示すブロック図である。

【図2】本発明の実施例として示す、デュアル暗号化オーディオデータをクリアなビデオデータとともに伝送するシステムの構成を示すブロック図である。

【図3】本発明の実施例として示す、番組の一部がタイムスライスメカニズムに基づいて、デュアル暗号化されるシステムの構成を示すブロック図である。

【図4】本発明の実施例として示す、デュアル暗号化処理のフローチャートである。

【図5】本発明の実施例として示す、暗号化処理のフローチャートである。

【図6】本発明の実施例として示す、番組の一部がパケット毎にデュアル暗号化されるシステムの構成を示すブロック図である。

【図7】本発明の実施例として示す、デュアル暗号化処理のフローチャートである。

【図8】本発明の実施例として示す、暗号化処理のフローチャートである。

【図9】本発明の実施例として示す、システム情報が暗号化され、番組がクリアな形式で伝送されるシステムの構成を示すブロック図である。

【図10】本発明の様々な実施例に対応する包括的なシステムの構成を示すブロック図である。

【図11】本発明の実施例として示す、ケーブルシステムヘッドエンドの第1の実現例を示すブロック図である。

【図12】本発明の実施例として示す、ケーブルシステムヘッドエンドの第2の実現例を示すブロック図である。

【図13】本発明の実施例として示す、ケーブルシステムヘッドエンドにおける暗号化処理のフローチャートである。

【図14】本発明の実施例として示す、セットトップボックスによって実現されたデコードシステムの第1の実現例を示すブロック図である。

【図15】本発明の実施例として示す、ケーブルシステムSTBによって実現されたデコードシステムの第2の実現例を示すブロック図である。

【図16】本発明の実施例として示す、ケーブルシステムSTBによって実現されたデコードシステムの第3の実現例を示すブロック図である。

【図17】本発明の実施例において、セットトップボックスPID再マッピング器により実行されるPID再マッピング処理を説明する図である。

【図18】本発明に基づくセットトップボックスにおいて用いられるデコーダチップの具体的構成例を示す図である。

【発明を実施するための形態】

【0018】

本発明は、数多くの異なる構成の実施例があるが、図面を参照して詳細に説明する特定の実施例は、開示内容が本発明の趣旨の一例とみなされるものであり、本発明をその特定の実施例に限定するものではない。後述する実施例において、類似の参照番号は、複数の図面における同じ、類似、又は対応する部分には、同じ参照番号を付している。用語「スクランブル(scramble)」、「暗号化(encrypt)」及びその活用形は、ここでは同義で用いられている。また、用語「テレビジョン番組(television program)」及び類似の用語は、日常会話に使用する意味とともに、テレビジョン受信機又は同様のモニタ装置に表示することができるA/Vコンテンツのいずれかのセグメントの意味にもなる。

【0019】

概要

現在のデジタルケーブルネットワークは、多くの場合、デジタルオーディオデータ及びビデオデータを完全に暗号化するC A方式を用いて、適切に申込みをした加入者以外は番組を視聴することができないようにしている。この暗号化は、ハッカー及び料金を払っていない未加入者が番組を受信することができないようにすることを目的としている。しかしながら、ケーブルテレビ運用業者は、加入者に複数のセットトップボックス製造業者のいずれの製品でも提供することができることを望んでいるため、それぞれのS T B製造業者のC A方式に対応した複数の暗号化技術を用いて、1つの番組を複数暗号化したコピーを送信しなければならない。

【0020】

番組の複数のコピーを伝送する（「フルデュアルキャリッジ」という。）必要があると、視聴者に更なる番組のコンテンツを提供することができる貴重な帯域幅も使い果たしてしまう。本発明の一実施例では、この問題に対応するために、複数のキャリッジと等価なもの（equivalent）を伝送するために必要な帯域幅を最小限に抑えるようにしてる。この結果、帯域全体を使用することなく、フルデュアルキャリッジと同等の効果を得ることができるので、この方式を「仮想デュアルキャリッジ（Virtual Dual Carriage）」と呼ぶ。本発明の幾つかの実施例では、部分的なスクランブルを効果的に実現する。どの部分を暗号化するかを選択する基準によって、様々な実施例がある。選択する部分によって、新たに必要とされる帯域幅と、暗号化の効果とが変わる。本発明の実施例に矛盾しない方法で、1つの暗号化処理又は複数の暗号化処理の組合せを用いることが好ましい。

【0021】

ここに開示する部分デュアル暗号化（partial dual encryption）では、複製された各コンポーネントに対して、追加的な（すなわち第2の）パケット識別子（P I D）を用いる。これらの第2のP I Dは、他の暗号化方法によって暗号化されたコンテンツのコピーを伝送するパケットのタグとして用いられる。番組特定情報（P S I）は、挿入された第2のP I Dが旧型のS T Bでは無視され、新型のS T Bでは容易に抽出することができるように、これら新しい第2のP I Dの存在に関する情報を伝送するように拡張されている。

【0022】

部分デュアル暗号化の実施例には、所定のP I Dを有するパケットのみを複製することにも含まれる。暗号化するパケットの選択方法は、後で詳述する。元の（すなわち旧）P I Dは、依然として、暗号化されずに（in the clear）送信されるパケットだけではなく、旧暗号化方式で暗号化されたパケットにもタグとして付される。新P I Dは、第2の暗号化方法によって暗号化されたパケットのタグとして用いられる。第2のP I Dが付けられたパケットは、第1のP I Dが付された暗号化パケットを隠す（shadow）。暗号化されたペアを構成する（making up）パケットは、いずれの順番で伝送されてもよいが、P I Dストリームの暗号化されていない部分のシーケンスを保つことが好ましい。以下の説明から明らかのように、第1と第2のP I Dを用いることにより、セットトップボックスに内蔵された復号器は、そのセットトップボックス自体の復号方法を用いて、どのパケットを復号するかを容易に判定することができる。P I Dの処理方法については後で詳細に説明する。

【0023】

ここに説明する暗号化技術は、（1つの分類方法として）大きく3つに、すなわち主要部（すなわちオーディオデータ）のみを暗号化する技術と、S Iのみを暗号化する技術と、選択されたパケットのみを暗号化する技術とに分類することができる。一般的に、ここに説明する実施例に用いられる各暗号化技術は、A / V信号の一部又は関連する情報を暗号化し、A / V信号の残りの部分をクリア（clear）にして帯域幅を節約する。帯域幅の節約が可能である理由は、同一のクリアな部分を、全ての種類のセットトップボックスに送信することができるためである。情報の暗号化する部分を選択するには、様々な方法が用いられる。これにより、本発明の様々な実施例では、1つの特定のスクランブル方式でコンテンツ全体を暗号化する従来の「強引な（brute-force）」、すなわち2つ以上のス

クランブル方式が望まれる場合において帯域を冗長に浪費する技術を用いないで済む。また、ここに説明する各部分デュアル暗号化方式は、本発明の実施例から逸脱することなく、1つの部分暗号化方式として用いることができる。

【0024】

本発明の様々な実施例では、複数の処理を単独又は組み合わせて用いて、コンテンツの実質的な部分(substantial portions)をクリアな形式で(暗号化せずに)に送り、一方、コンテンツを正しく再生するのに必要とされるデータ量の少ない情報のみを暗号化する。したがって、所望の各番組ストリームの全体をコピーするのに対し、特定のスクランブル方式で独自に暗号化され、伝送される情報量は、コンテンツのほんの一部である。この明細書における具体的なシステムでは、暗号化方式Aは旧式であるとみなしている。上述した幾つかの暗号化技術を、以下に詳細に説明する。

【0025】

本発明の様々な実施例において用いられる各CA方式は、独立して動作することができる。各CA方式は、他の方式と直交している。各CA方式は、それ自体のパケットを暗号化するので、ヘッドエンドにおける鍵の共用は不要である。各CA方式において、異なる暗号鍵方式(different key epochs)を用いてもよい。例えば、モトローラ社所有の暗号化方式によって暗号化されたパケットは、組み込みセキュリティASICによって発生された高速変更暗号鍵(fast changing encryption keys)を用いることができ、一方、NDS社のスマートカードベースの方式で暗号化されたパケットは、それより僅かに遅い変更暗号鍵を用いることができる。この実施例のシステムは、サイエンティフィックアトランタ社及びモトローラ社の旧式の暗号化方式に対しても同等にうまく動作する。

【0026】

暗号化エレメンタリストリーム(ENCRYPTED ELEMENTARY STREAM)

図2に示すシステム100は、複数のキャリアジを提供するために帯域幅を追加する必要性を減らすシステムの一実施例である。この実施例において、システム100は、音声を聞かないでテレビジョン番組を見ることは普通好まれないという事実を利用している。例外(例えば成人番組、ある種のスポーツ競技番組等)はあるが、一般的な視聴者は、日常、音声を聞くことができないでテレビジョン番組を見ることは受け入れ難い。したがって、ヘッドエンド122において、ビデオデータ104はクリアに(暗号化しないで)ケーブルネットワークを介して放送するが、クリアなオーディオデータ106は複数のCA装置に供給した後、放送する。具体的なシステム100においては、クリアなオーディオデータ106は、暗号化方式Aを用いてオーディオデータを暗号化する暗号化装置118に供給される(暗号化方式Aは、この明細書中では旧式の暗号化方式とする)。同時に、クリアなオーディオデータ106は、暗号化方式Bを用いてオーディオデータを暗号化する暗号化装置124に供給される。そして、クリアなビデオデータには、暗号化装置118、124からの暗号化されたオーディオデータ(オーディオA、オーディオB)と、システム情報128と、番組特定情報129とが多重化される。

【0027】

ビデオデータ、システム情報、番組特定情報、オーディオA及びオーディオBの全ては、ケーブルシステム32を介して配信された後、セットトップボックス(STB)36、136で受信される。旧型のSTB36において、ビデオデータはテレビジョン受信機44で表示され、暗号化オーディオデータは、CA方式A40によって復号され、テレビジョン受信機44で再生される。同様に、新型のSTB136において、ビデオデータはテレビジョン受信機144で表示されるとともに、暗号化オーディオデータは、CA方式B140によって復号され、テレビジョン受信機144で再生される。

【0028】

オーディオデータは、完全なA/Vプログラムに比して(又はビデオデータのみ部分と比べても)、必要とされる帯域幅は相対的に少ない。ステレオのオーディオデータを384kb/sで送信する場合、現在の最大ビットレートは、3.8Mb/sのテレビジョン番組の約10%である。したがって、256QAM(直交振幅変調)で送られる10チ

チャンネルのシステムにおいて、暗号化オーディオデータのみデュアルキャリッジ（ビデオデータは暗号化しないで伝送される）では、約1チャンネル分の帯域幅の損失（loss）しか発生しない。したがって、約9チャンネルを送信することができる。このことは、全てのチャンネルをデュアル暗号化する必要があり、送信可能なチャンネル数が10から5に減少する場合に比して、大幅な改善である。なお、例えばスポーツ競技の番組、ペイパービューの番組、成人番組等において、必要がある場合には、オーディオデータとビデオデータの両方を、今まで通りデュアル暗号化することもできる。

【0029】

旧型のセットトップボックスと新型のセットトップボックスの両方とも、クリアなビデオデータを通常の方法で受信するとともに、暗号化A/Vコンテンツを完全に復号するのに用いられる方法と同じ方法で、オーディオデータを復号するように機能することができる。ユーザが、上述した方法で暗号化された番組を視聴する申込みをしていない場合、ユーザは、良くて、音声を聞かないで映像を見ることができるだけである。ビデオデータのセキュリティを上げるためには、ここで本発明の（後述する）他の実施例を用いることもできる。（例えば、SIにスクランブルを掛けて、未許可のセットトップボックスが番組のビデオデータ部分を選局することが難しくなるようにしてもよい。）未許可であって、ハッカーによって改造されていないセットトップボックスは、暗号化オーディオデータを受信すると、映像を消して（blank）しまう。

【0030】

許可されたセットトップボックスは、アクセス基準（access criteria）及びデスクランブル鍵を受け取るために用いられる資格制御メッセージ（Entitlement Control Message：以下ECMという。）を受信する。このセットトップボックスは、デスクランブル鍵をオーディオデータだけでなく、ビデオデータに対しても適用する。ビデオデータは、スクランブルが掛かっていないので、セットトップボックスのデスクランブラをそのまま通過する。セットトップボックスは、ビデオデータがクリアあるかを考慮しない。未改造（un-modified）且つ未加入（un-subscribed）のセットトップボックスは、クリアなビデオデータとスクランブルが掛かったオーディオデータに対して、未許可（un-authorized）のセットトップボックスとして動作する。オーディオデータだけではなく、ビデオデータにも実際にスクランブルが掛かっている場合には、映像は表示されない。そして、画面上に、視聴者が番組を視聴するためには申込みが必要であることを示すオンスクリーンディスプレイが現れるようにしてもよい。これにより、視聴者が偶然、コンテンツを聞くことと、見ることの両方を完全に防止することができる。

【0031】

本発明の一実施例において、暗号化オーディオデータは、デジタルパケットとしてA/Vチャンネルを介して配信される。2つ（又は2つ以上）のオーディオストリームは、システム100のセットトップボックスで採用されている2つ（又は2つ以上）の暗号化方式に基づいてそれぞれ暗号化されて、伝送される。2つ（又は2つ以上）のSTBにおいて、それぞれのオーディオストリームを適切に復号及びデコードするために、システム100のヘッドエンド122から、伝送サービス識別子（Service Identifier）を用いてオーディオデータが位置するチャンネルを検出するためのSI（システム情報）データが送信される。この処理は、CA方式A40のオーディオデータに対して第1のパケット識別子（PID）を割り当て、CA方式B140のオーディオデータに対して第2のパケット識別子（PID）を割り当てることにより実現される。限定されるものではないが、一具体例として、以下の番組特定情報（PSI）を、NDS社とモトローラ社の限定受信技術をそれぞれ用いた2つのCA方式におけるオーディオデータの位置を指定するために送ってもよい。この番組特定情報を後述する部分暗号化の他の実施例に適用できることは、当業者に明らかである。

【0032】

SIは、旧型のセットトップボックスと非旧型のセットトップボックスの両方に別々に送信することができる。また、SIは、旧型のセットトップボックスと非旧型のセットト

ップボックスが基本的に混信することなく動作するように、送信することができる。旧型のセットトップボックスに配信されるS I内の仮想チャンネルテーブル(virtual channel table: V C T)は、所望の番組、例えばプログラム番号1として参照されるH B OはサービスIDが「1」であり、V C Tアクセス制御ビットが設定されていることを示している。旧型のセットトップボックスに配信されるネットワーク情報テーブル(network information table: N I T)は、サービスID「1」が周波数1 2 3 4であることを示している。また、非旧型のセットトップボックスに配信されるS I内のV C Tは、所望の番組、例えばプログラム番号1 0 0 1で参照されるH B OはサービスIDが「1 0 0 1」であり、V C Tアクセス制御ビットが設定されていることを示している。非旧型のセットトップボックスに配信されるN I Tは、サービスID「1 0 0 1」が周波数1 2 3 4であることを示している。以下に例示的に示す放送番組関連テーブル(program association table: P A T)のP S Iデータは、旧型と非旧型のセットトップボックスの両方に(M P E Gデータ構造フォーマットで)送信される。

【 0 0 3 3 】

【表 1】

PID=0x0000 で伝送される PAT
PAT 0x0000
- トランスポートストリーム ID
- PAT バージョン
- 番組番号 1
- PMT 0x0010
- 番組番号 2
- PMT 0x0020
- 番組番号 3
- PMT 0x0030
- 番組番号 4
- PMT 0x0040
- 番組番号 5
- PMT 0x0050
- 番組番号 6
- PMT 0x0060
- 番組番号 7
- PMT 0x0070
- 番組番号 8
- PMT 0x0080
- 番組番号 9
- PMT 0x0090
- 番組番号 1 0 0 1
- PMT 0x1010
- 番組番号 1 0 0 2
- PMT 0x1020
- 番組番号 1 0 0 3
- PMT 0x1030
- 番組番号 1 0 0 4
- PMT 0x1040
- 番組番号 1 0 0 5
- PMT 0x1050
- 番組番号 1 0 0 6
- PMT 0x1060
- 番組番号 1 0 0 7
- PMT 0x1070
- 番組番号 1 0 0 8
- PMT 0x1080
- 番組番号 1 0 0 9
- PMT 0x1090

【 0 0 3 4 】

以下の具体的な放送番組マップテーブル (program map table: PMT) の P S I データは、旧型及び非旧型のセットトップボックスによって (MPEG データ構造フォーマットで) 選択的に受信される。

【 0 0 3 5 】

【表 2】

<p>PID=0x0010 で伝送される PMT</p> <p>PMT 0x0010</p> <ul style="list-style-type: none"> - PMT 番組番号 1 - PMT セクションバージョン 1 0 - PCR PID 0x0011 - エレメンタリストリーム <ul style="list-style-type: none"> - ストリームタイプ (ビデオ 0x20 又は 0x80) - エレメンタリ PID (0x0011) - 記述子 <ul style="list-style-type: none"> - CA プロバイダ # 1 用の CA 記述子(ECM) - エレメンタリストリーム <ul style="list-style-type: none"> - ストリームタイプ (オーディオ 0x81) - エレメンタリ PID (0x0012) - 記述子 <ul style="list-style-type: none"> - CA プロバイダ # 1 用の CA 記述子(ECM)
<p>PID=0x1010 で伝送される PMT</p> <p>PMT 0x1010</p> <ul style="list-style-type: none"> - PMT 番組番号 1 0 1 0 - PMT セクションバージョン 1 0 - PCR PID 0x0011 - エレメンタリストリーム <ul style="list-style-type: none"> - ストリームタイプ (ビデオ 0x02 又は 0x80) - エレメンタリ PID (0x0011) - 記述子 <ul style="list-style-type: none"> - CA プロバイダ # 2 用の CA 記述子(ECM) - エレメンタリストリーム <ul style="list-style-type: none"> - ストリームタイプ (オーディオ 0x81) - エレメンタリ PID (0x0013) - 記述子 <ul style="list-style-type: none"> - CA プロバイダ # 2 用の CA 記述子(ECM)

【 0 0 3 6 】

NDS社のCA方式に加えて、モトローラ社とサイエンティフィックアトランタ社のいずれかのCA方式を採用したシステムにおいて、番組の配信に適した一具体例では、上述の通信は、少し変更するだけで、モトローラ社とサイエンティフィックアトランタ社の両方のCA方式で配信されるPSIとは矛盾しない。放送番組関連テーブル(PAT)は、各番組の追加的な放送番組マップテーブル(PMT)を参照するように変更される。この実施例において、各番組は、PAT内にそれぞれ2つのプログラム番号を有する。上記表1において、プログラム番号1及びプログラム番号1001は、同じ番組であるが、それぞれ異なる音声PID及びCA記述子を参照している。システム100において、複数のPMTを生成するとともに、新たなPAT及びPMTの情報をデータストリームに多重化する変更は、ケーブルシステム32のヘッドエンド装置を適切に変更することによって、行うことができる。また、これらのメッセージを明細書に記載の他の部分暗号化方式により暗号化できることは、当業者に明らかである。この方法では、ヘッドエンド、又は旧型及び非旧型のセットトップボックスに特別なハードウェア又はソフトウェアを必要とせず、この方法を用いて旧式と非旧式の暗号化方式で暗号化されたオーディオ信号を配信することができるという利点がある。

【 0 0 3 7 】

この技術により、ユーザが料金を支払っていない有料番組の音声を聞こえないようにして視聴を阻止することができるが、ハッカーは、映像を選局することができる。これに対抗するために、本発明の他の暗号化技術において用いられる（後述するような）機構（mechanisms）を、必要に応じて同時に使用してもよい。一般的に、文字多重情報はビデオデータの一部として伝送されているので、ユーザは、クリアな映像とともに、読める音声情報を得ることができる。したがって、この技術は、ある用途には向いているが、全ての用途に対しては、単独では十分な保護を与えとは言えない。他の実施例において、ペイロードの一部として文字多重情報を含むビデオパケットに、更にスクランブルを掛けてもよい。

【0038】

他の実施例において、ビデオデータのみをデュアル又は多重暗号化して、暗号化ビデオデータの各セットに別々のPIDを割り当ててもよい。これにより、（ビデオデータはオーディオデータより重要であるので）通常番組に対してより堅固な暗号化を提供することができるが、全てのセットトップボックスで共用されるのはオーディオデータのみであるので、節約できる帯域幅の量は、フルデュアルキャリッジに比べて僅かに約10%である。なお、この方法を、例えば成人番組及びスポーツ競技番組等のある特定のコンテンツに用いて、そのコンテンツに対する帯域幅のオーバーヘッドを削減し、他の種類のコンテンツに対してはオーディオ暗号化方法を用いてもよい。ディレクTV（DirecTV、商標）サービスで用いられているデジタル衛星サービス（Digital Satellite Service：DSS）のトランスポート規格（transport standard）においてパケット識別子と同等なものとみなされるサービスチャンネル識別子（service channel identifier：SCID）を用いて、オーディオパケットの暗号化を識別することができる。

【0039】

タイムスライシング

本発明の他の実施例は、タイムスライシングに関し、システム200として図3に示す。この実施例においては、各番組の一部を時間依存ベースで暗号化して、ユーザが番組視聴の支払いをしていないときには、番組の視聴を中止させる。本発明のこの実施例は、ビデオデータを部分的に暗号化するとともにオーディオデータをクリアなものとする、ビデオデータをクリアなものとするとともにオーディオデータを部分的に暗号化する、或いはビデオデータ及びオーディオデータを部分的に暗号化することによって実現することができる。タイムスライス、すなわち暗号化されている期間の全時間に対する割合は、使用される帯域幅とハッカーに対する安全性とのバランスが最適になるように、選択することができる。一般的に、ここに述べるどの実施例においても、コンテンツを100%未満で暗号化して、所望の部分暗号化データを生成している。以下の具体例において、ビデオデータ及びオーディオデータの部分暗号化について説明する。

【0040】

一例として、且つこれに限定されるものではないが、本発明の具体的な実施例に基づいて9つの番組をデュアル部分暗号化（dual partially encrypt）システムを説明する。これらの9チャンネルは、パケットの多重化されたストリームとして、ケーブルヘッドエンド222に供給され、9つの番組のうち特定の1つの番組に関連したパケットを識別するためのパケット識別子（PID）を用いてデジタル的にエンコードされる。この具体例において、これら9つの番組は、101～109の番号が付けられたビデオPIDと、201～209の番号が付けられたオーディオPIDとを有しているとする。この実施例に基づいた部分暗号化は、任意の時間においては1つの番組のパケットのみが暗号化されるように、9つの番組に対して時分割的に行われる。この方法は、コンテンツが分かっている（content-aware）必要はない。

【0041】

下記表3を参照して、本発明の実施例であるタイムスライスデュアル暗号化を説明する。第1のビデオPID101及び第1のオーディオPID201を有する番組1について、第1の期間ではPID101及びPID201を有するパケットを暗号化方式Aを用い

て暗号化し、他の番組を表す他のパケットをクリアに送信する。この実施例において、第2のPIDもビデオパケット及びオーディオパケットに対して割り当てられている。番組1の第2のPIDは、ビデオパケットに対してはPID 111であり、オーディオパケットに対してはPID 211である。第2のPIDが割り当てられたパケットを、第1の期間では暗号化方式Bを用いて暗号化し、次の8期間ではクリアに送信する。そして、期間10において、上述した4つのPIDのいずれかを有するパケットを再び暗号化し、続く8期間ではクリアに送信する。同様に、第1のビデオPID 102及び第1のオーディオPID 202を有する番組2を、期間2において、暗号化方式Aを用いて暗号化し、対応する第2のPIDが割り当てられたパケットを、暗号化方式Bを用いて暗号化し、次の8期間ではクリアに送信し、以下同様とする。このパターンは、表3の最初の9行から明らかである。この技術によって、本発明を逸脱することなく、オーディオパケットとビデオパケットの両方を、オーディオパケットのみを、或いはビデオパケットのみを暗号化することができる。また、オーディオパケットとビデオパケットは、それぞれ個別の暗号化シーケンスを有することができる。表3において、P1は期間1、P2は期間2を示し、以下同様である。EAは、情報がCA方式Aを用いて暗号化されることを示し、EBは、情報がCA方式Bを用いて暗号化されることを示す。

【0042】

【表 3】

番組	ビデオ PID	オーディオ PID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	...
1	PID 101	PID 201	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	...
2	PID 102	PID 202	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
3	PID 103	PID 203	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
4	PID 104	PID 204	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
5	PID 105	PID 205	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
6	PID 106	PID 206	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	...
7	PID 107	PID 207	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	...
8	PID 108	PID 208	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	...
9	PID 109	PID 209	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	...
1	PID 111	PID 211	EB									EB			...
2	PID 112	PID 212		EB									EB		...
3	PID 113	PID 213			EB									EB	...
4	PID 114	PID 214				EB									...
5	PID 115	PID 215					EB								...
6	PID 116	PID 216						EB							...
7	PID 117	PID 217							EB						...
8	PID 118	PID 218								EB					...
9	PID 119	PID 219									EB				...

【 0 0 4 3 】

従来の旧式の暗号化方式（暗号化方式 A）と互換性を保つために、暗号化期間では、各番組 1～9 を暗号化方式 A を用いて暗号化する。旧型の S T B 装置は、このように部分暗号化された A / V データストリームを受信し、透過的に、暗号化されていないパケットを通過し、暗号化されているパケットを復号する。しかしながら、暗号化方式 A と暗号化方式 B の両方を用いたデュアル暗号化方式の方が望ましい。デュアル暗号化を行うために、

特定の有料番組には、第1のPID（例えば番組1に対してはビデオPID101及びオーディオPID201）と第2のPID（例えば番組1に対してはビデオPID111及びオーディオPID211）の両方が割り当てられ、特定の有料チャンネルのエレメンタリデータストリーム（elementary data stream）が送信される。

【0044】

図3は、システム200におけるケーブルシステムヘッドエンド222の機能（functionality）を概略的に示すブロック図であり、ヘッドエンド222において、Nチャンネルのクリアなビデオパケット208は、インテリジェントスイッチ216（プログラミングされたプロセッサの制御下で動作する）に供給され、インテリジェントスイッチ216は、クリアに伝送するパケットをPID割当器220に供給し、PID割当器220は、これらのパケットに第1のPIDを割り当てる。暗号化されるパケットは、CA方式A暗号化器218とCA方式B暗号化器224の両方に供給される。CA方式A暗号化器218とCA方式B暗号化器224は、これらのパケットをそれぞれ暗号化して、PID割当器220に供給し、PID割当器220は、それぞれ第1のPID又は第2のPIDを割り当てる。クリアなパケット、CA方式Aの暗号化パケット、CA方式Bの暗号化パケット、システム情報228及びPSI229は多重化又は組み合わせられ、ケーブルシステム32を介して放送される。

【0045】

説明のために、タイムスライスの期間を100msとすると、表3に示すように、平均して1.1(one and a fraction)の暗号化期間があり、合計して全9番組について毎秒111msとなる。タイムスライスの期間を50msとすると、平均して2.1の暗号化期間があり、合計して111msとなる。未加入のセットトップボックスで、ビデオ信号に選局しようとした場合、如何なる画像に固定できたとしても、非常に悪い画質の画像しか得られず、音声は不明瞭なものになってしまう。

【0046】

部分スクランブルされたストリームのPSIは、上述した具体例のデュアルオーディオ暗号化における場合と僅かに異なって処理される。基本的には、旧型のセットトップボックスと非旧型のセットトップボックスの両方に、同じSI及びPATのPSI情報を送信することができる。異なるのは、PMTのPSI情報である。旧型のセットトップボックスは、PMTのPSIを解析して、従前の第1のビデオPID及びオーディオPIDを得る。非旧型のセットトップボックスは、旧型のセットトップボックスと同様に第1のPIDを得るが、データストリームが部分的にスクランブルされているか否かを確認するために、PMTのPSI内のCA記述子を調べなければならない。特定のCAプロバイダは、第2のPIDを故意にスクランブルしており、したがって、そのPIDを送るためには、特定のCAプロバイダ固有のCA記述子を用いる。本発明では、2つ以上の第2のPIDを用いることができるようにすることによって、複数のCAプロバイダを共存させることができる。第2のPIDは、特定のCAプロバイダに対して固有のものである。セットトップボックスは、それ自体が有しているCA方式のCAIDを知っており、そのCA方式に関連した全てのCA記述子を確認することができる。

【0047】

第2のPIDを、ECMで用いられているのと同じCA記述子内のプライベートデータとして送信できるが、好ましい実施例においては、別のCA記述子を用いる。第2のPIDは、CA PIDフィールド内に配置されている。これにより、ヘッドエンド処理装置は、CA記述子のプライベートデータフィールドを解析することなく、PIDを「調べる（see）」ことができる。ECMのCA記述子と第2のPIDのCA記述子との違いは、第2のPIDのCA記述子では、ダミーのプライベートデータ値を送信することができることである。

【0048】

【表 4】

<p>PID=0x0010 で伝送される PMT</p> <p>PMT 0x0010</p> <ul style="list-style-type: none"> -PMT 番組番号 1 -PMT セクションバージョン 1 0 -PCR PID 0x0011 -エレメンタリストリーム <ul style="list-style-type: none"> -ストリームタイプ (ビデオ 0x02 又は 0x80) -エレメンタリ PID (0x0011) -記述子 <ul style="list-style-type: none"> -CA プロバイダ # 1 用の CA 記述子(ECM) -CA プロバイダ # 2 用の CA 記述子(ECM) -CA プロバイダ # 2 用の CA 記述子(第 2 の P I D) -エレメンタリストリーム <ul style="list-style-type: none"> -ストリームタイプ (オーディオ 0x81) -エレメンタリ PID (0x0012) -記述子 <ul style="list-style-type: none"> -CA プロバイダ # 1 用の CA 記述子(ECM) -CA プロバイダ # 2 用の CA 記述子(ECM) -CA プロバイダ # 2 用の CA 記述子(第 2 の P I D)

【 0 0 4 9 】

【表 5】

CA プロバイダ # 2 用の CA 記述子(ECM)

<p>記述子</p> <ul style="list-style-type: none"> -タグ：限定受信 (0x09) -長さ：4 バイト -データ <ul style="list-style-type: none"> -CA 方式 ID：0x0942 (第 2 の CA プロバイダ) -CA PID (0x0015)

【 0 0 5 0 】

【表 6】

CA プロバイダ # 2 用の CA 記述子(第 2 の P I D)

<p>記述子</p> <ul style="list-style-type: none"> -タグ：限定受信 (0x09) -長さ：5 バイト -データ <ul style="list-style-type: none"> -CA 方式 ID：0x1234 (第 2 の CA プロバイダ) -CA PID (0x0016) -プライベートデータ

【 0 0 5 1 】

CA 方式 A に基づいて動作する旧型の STB 36 は、データを受信すると、第 2 の PID を無視し、CA 方式 A によって暗号化されたパケットを復号し、テレビジョン受信機 44 に番組を表示する。非旧型の、すなわち新型の STB 236 は、SI 228 を受信する。新型の STB 236 は、PSI 229 を受信し、PMT を用いて、第 2 の CA 記述子内

から読み出され、視聴する番組に関連した第1及び第2のPIDを識別する。CA方式Aによって暗号化されたパケットは破棄され、CA方式Bによって暗号化され、第2のPIDを有するパケットは、CA方式B240によって復号され、デコード及びテレビジョン受信機244に表するために、クリアなデータストリーム内に挿入される。

【0052】

図4は、本発明の実施例を実現するために用いることができるケーブルシステムのヘッドエンドにおけるエンコード処理を示す図であり、CA方式Aは、旧式の方式であり、CA方式Bは、導入される新しい方式である。ステップ250において、所定の番組がクリアなパケットとして供給されると、そのパケット(又はフレーム)が暗号化されない(すなわち、暗号化の現在のタイムスライスが、この番組に対するものでない)ときは、ステップ254において、クリアなパケット(C)は、出力ストリームに挿入される。現在のパケットが、暗号化タイムスライスの一部であることにより暗号化されるときには、パケットは、パケット暗号化処理Aのステップ258とパケット暗号化処理Bのステップ262において、それぞれ暗号化される。ステップ258における暗号化処理A(EA)で暗号化されたパケットは、ステップ254において、出力ストリームに挿入される。ステップ262における暗号化処理B(EB)で暗号化されたパケットは、ステップ264において、第2のPIDが割り当てられ、ステップ254において、出力ストリームに挿入される。この処理が番組内の全てのパケットに対して繰り返される。

【0053】

図5は、新たに導入されたCA方式Bを有するSTB236において用いられる、上述した第1及び第2のPIDを有するCパケット、EAパケット及びEBパケットを含む受信データストリームを復号及びデコードする処理を示す。ステップ272において、パケットが受信されると、そのパケットに所定の第1のPIDがあるか否かが調べられる。第1のPIDがないときには、ステップ274において、そのパケットに所定の第2のPIDがあるか否かが調べられる。第1のPIDと第2のPIDのいずれもないときには、このパケットは、ステップ278において、無視或いは破棄される。第1のPID又は第2のPIDでないEAパケットとEBパケット間の如何なるパケットも、破棄される。デコーダが、常にEBパケットを受信する前にEAパケットを受信し、又は常にEAパケットを受信する前にEBパケットを受信することができるかは、設計事項及びバッファリングの問題である。また、第2のパケットを、第1のパケットの後ではなく前に検出するように設計することは、同様に容易である。また、第2のパケットを第1のパケットの前又は後のいずれにおいても受信できるように、回路を設計することは可能である。パケットに所定の第1のPIDがある場合、ステップ284において、パケットが暗号化されているか否かが判定される。暗号化されていない場合、そのパケット(C)は、ステップ288において、直ちにデコーダに供給され、デコードされる。ステップ284においてパケットが暗号化されていると判定された場合、そのパケットは、EAパケットであるとみなされ、ステップ278において、破棄或いは無視される。ある実施例において、第1のパケットの暗号化は、ステップ284において調べない。むしろ、ステップ284において、第1(第2)のパケットの第2(第1)のパケットに対する位置を単に検出して、第1(第2)のパケットを識別することもできる。

【0054】

ステップ274において、パケットが第2のPIDを有する場合、第2のPIDは、ステップ292において、第1のPIDに再マッピングされる(或いは、同等に、第1のPIDは、第2のPID値に再割当てされる)。そして、パケットは、ステップ296において復号され、ステップ288においてパケットデコーダに供給され、デコードされる。言うまでもないが、本発明から逸脱することなく、様々の変更が可能であることは、当業者に明らかであり、例えば、ステップ292とステップ296の順番又はステップ272とステップ274の順番は入れ替えることができる。先に述べたように、ステップ284は、第2のパケットに対する第1のパケットの位置の検出に置き換えることができる。当業者は、他の変更を想到することもできる。

【 0 0 5 5 】

暗号化方式 A によって動作する旧型の S T B 3 6 は、第 2 の P I D のパケットを完全に無視する。第 1 の P I D を有するパケットは、必要に応じて復号され、クリアなパケットのときは、復号されずにデコードに供給される。したがって、暗号化方式 A によって動作する所謂「旧型の」S T B は、第 1 の P I D に関連した部分暗号化データストリームを適切に復号及びデコードし、第 2 の P I D のデータストリームを変更することなく、無視する。暗号化方式 B によって動作する S T B は、第 1 の P I D に関連した全ての暗号化パケットを無視し、特定のチャンネルに関連した第 2 の P I D を有する、伝送されてきた暗号化パケットを用いるようにプログラミングされている。

【 0 0 5 6 】

したがって、各デュアル部分暗号化された番組は、2 セットの P I D を有する。暗号化が、上述のように適切なタイムスライス間隔によって示されるシステムに対して期間ベースで実行されるときには、いずれの復号方式を有する S T B においても、画像は基本的に見ることができない。

【 0 0 5 7 】

図 6 に示すヘッドエンド 3 2 2 においてこのシステムを実現するために、S I 及び P S I は、C A 記述子情報の第 2 のセットを含むように変更することができる。旧型の S T B は、未知の C A 記述子を許容することができない。したがって、代わりに、旧型の S T B において、コンテンツ P I D 及び / 又は S I / P S I と、E C M の P I D との両方に対して、旧式 C A P I D からのオフセットを「ハードコーディング (hard code)」することができるようにしてもよい。或いは、パラレル P S I を送ってもよい。例えば、非旧型の S T B に対しては、P I D 0 ではなく、P I D 1 0 0 0 で補助的な P A T を配信することができる。非旧型の S T B は、旧 P A T 内にはない補助的な P M T を参照することができる。補助的な P M T は、非旧式の C A 記述子を含むことができる。補助的な P M T は、旧型の S T B には知られていないので、同時に使用 (interoperation) の問題は生じない。

【 0 0 5 8 】

モトローラ社又はサイエンティフィックアトランタ社によって製造された旧型の S T B に対応した方式 A のシステムにおいては、S T B は何ら変更する必要はない。一方、方式 B 対応の S T B においては、ここに説明する部分暗号化された番組のデュアルキャリッジに対して、ビデオ及びオーディオデコードは、それぞれ 1 つのみではなく、それぞれ 2 つの P I D (第 1 の P I D 及び第 2 の P I D) を参照する (listen)。使用する新 C A 方式の数によって、1 つ以上の第 2 のシャドウ P I D (shadow PID) があるが、特定の S T B は、そこに用いられている C A 方式に適した 1 つの第 2 の P I D しか参照 (listen) しない。また、ほとんどがクリアなビデオデータ又はクリアなオーディオデータを伝送している (carrying) P I D からの暗号化パケットは無視することが理想的である。「不適合パケット (bad packets)」(そのまま簡単にデコードできないパケット) を無視することは、多くのデコードにおいて既に実行されている機能であるので、変更の必要はない。不適合パケットを無視しないデコードを用いたシステムにおいては、フィルタ機能を用いることができる。なお、タイムスライス暗号化技術は、ビデオデータ及びオーディオデータにしか適用することができない。また、上述の実施例に示したように、ビデオデータはタイムスライス暗号化され、一方、オーディオデータはデュアル暗号化される。タイムスライス暗号化技術は、複数の番組に同時に適用することができる。ある期間に暗号化される番組の数は、帯域幅の割当てによって異なり、ここでは一度に 1 つの番組をスクランブルする例を記載しているが、本発明はこれに限定されるものではない。本明細書に記載の暗号化技術の他の組合せも、当業者に明らかである。

【 0 0 5 9 】

M 番目 N パケット暗号化

本発明の他の実施例として、「M 番目 N パケット暗号化 (Mth & N packet encryption)」を説明する。これは、図 3 にシステム 2 0 0 として示す実施例の変形例である。この実施例では、それぞれ 1 つの番組を表す P I D のパケットは、ユーザが番組の料金を払っ

ていない場合には、ユーザが番組を視聴できないように暗号化する。この実施例において、Mは、各暗号化イベント(event)の開始点間にあるパケットの数を表し、Nは、暗号化が一度開始してから連続して暗号化されるパケットの数を表す。NはMよりも小さい数である。M = 9 且つ N = 1 ならば、9 パケット毎に1 パケット連続した暗号化イベントがある。M = 16 且つ N = 2 ならば、16 パケット毎に2 パケット連続した暗号化イベントがある。上述の実施例のように、デュアル部分暗号化される各パケットは、CA方式A 2 1 8 及びCA方式B 2 2 4 を用いて複製及び処理される。この実施例と上述のタイムスライス暗号化技術との動作における違いは、スイッチ2 1 6 の動作によって、プログラミングされたプロセッサの制御下で暗号化するパケットを選択することにある。

【0060】

本発明は、これに限定されるものではないが、この実施例によってデュアル暗号化される9チャンネルの番組を有するシステムを説明する。これらの9個のチャンネルは、9個の番組の内の特定の1番組に対応するパケットを識別するパケット識別子(PID)を用いてデジタル符号化される。この具体例では、これらの9個の番組は、番号101~109のビデオPID及び番号201~209のオーディオPIDを有することとする。この実施例における暗号化は、番組間でランダム(random program-to-program)であり、他の番組からのパケットを同時に暗号化してもよい。この具体例は、M = 6 且つ N = 2 であり、ビデオパケットのみを暗号化する例である下表7に示されるが、これは本発明を限定するものではない。この方法は、コンテンツウェアである必要はない。表7において、PK1はパケット番号1を表し、PK2はパケット番号2を表し、以下同様である。

【0061】

【表 7】

番組	ビデオ	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
1	PID 101	EA	クリア	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	...
2	PID 102	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	...
3	PID 103	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	...
4	PID 104	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	...
5	PID 105	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	...
6	PID 106	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	...
7	PID 107	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	...
8	PID 108	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	...
9	PID 109	EA	クリア	クリア	クリア	クリア	EA	EA	クリア	クリア	クリア	クリア	EA	...
1	PID 111	EB	EB					EB	EB					...
2	PID 112				EB	EB					EB	EB		...
3	PID 113			EB	EB					EB	EB			...
4	PID 114				EB	EB					EB	EB		...
5	PID 115			EB	EB					EB	EB			...
6	PID 116	EB					EB	EB					EB	...
7	PID 117	EB	EB					EB	EB					...
8	PID 118		EB	EB					EB	EB				...
9	PID 119	EB					EB	EB					EB	...

【0062】

表 7 に示す具体例では、各番組は、 $M = 6$ 且つ $N = 2$ の暗号化方式を用いて他の番組から完全に独立して暗号化される。ここでも、ビデオパケットのみを暗号化する例を示しているが、この実施例又は他の変形例において、オーディオパケットも暗号化してもよい。ビデオパケットのみにこの暗号化を適用した場合、オーディオパケットは、上述の実施例と同様に、デュアル暗号化又はタイムスライス暗号化してもよい。或いは、オーディオパケットのみにこの暗号化を適用する場合、ビデオパケットは、上述の実施例と同様に、タイムスライシングしてもよい。

【0063】

本明細書に開示する部分スクランブルの概念に対応する技術を様々に変形できることは当業者には明らかである。例えば、5個のクリアなパケットの次に2個の暗号化パケット、2個のクリアなパケット、1個の暗号化パケットと続くパターン(C C C C C E E C C E C C C C C E E C C E . . .)は、本発明の部分暗号化概念の変形例であり、暗号化するパケットの選択のために、M及びNのランダム値、疑似ランダム値又はセミランダム値を用いてもよい。パケットのランダム、疑似ランダム又はセミランダム(全てを含めて「ランダム」という。)に選択することにより、ハッカーが、ポストプロセッシング(post processing)において、パケットをアルゴリズム的に再構築して、記録されたスクランブルコンテンツを再生することが困難になる。後述する部分暗号化の他の実施例にこの情報を適用する手法は、当業者に明らかである。幾つかの実施例は、組み合わせて用いることにより、コンテンツの安全性をより高めることができる。

【0064】

データ構造暗号化

本発明の実施例である他の部分暗号化方法では、データ構造毎に暗号化を行う。例えば、暗号化を好適に適用できるデータ構造の1つは、MPEGビデオフレームであるが、これに限定されるものではない。この具体例は、表8に示す具体例では、ビデオフレームを10フレーム毎に1フレーム暗号化する(ここでも、ビデオフレームのみを暗号化する)が、これは本発明を限定するものではない。この実施例では、各番組の10フレーム毎の暗号化サイクルは、それぞれのチャンネル毎に別個であるが、これは本発明を限定するものではない。この概念は、ビデオフレーム又はオーディオフレーム(或いは他の何らかのデータ構造)を基礎とし、例えば $M = 10$ 且つ $N = 1$ である、タイムスライシング又はM番目N部分暗号化配列(又は他のパターン)の変形例である。勿論、M及びNの他の値も同様の実施例において用いることができる。表8において、F1はフレーム番号1、F2はフレーム番号2を表し、以下同様である。

【0065】

【表 8】

番組 番号	ビデオ	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
1	PID 101	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
2	PID 102	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
3	PID 103	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
4	PID 104	クリア	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
5	PID 105	クリア	クリア	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	...
6	PID 106	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
7	PID 107	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
8	PID 108	クリア	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	...
9	PID 109	EA	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	クリア	EA	クリア	...
1	PID 111	EB										EB		...
2	PID 112				EB									...
3	PID 113			EB										...
4	PID 114					EB								...
5	PID 115													...
6	PID 116	EB										EB		...
7	PID 117		EB										EB	...
8	PID 118		EB										EB	...
9	PID 119	EB										EB		...

【0066】

したがって、ここでも、暗号化された番組は、それぞれ対応する2セットのPIDを付加されている。暗号化が上述のように、図に示すシステムに対して期間毎に実行された場合、画像は基本的に見ることができない。1秒間に30フレームを表示する9番組方式(nine program system)では、1秒間におよそ3フレームを暗号化する。番組視聴の権利を有さない視聴者のSTBが継続的に同期及び再生を試みても、部分的な静止画像を取得することしかできない。番組視聴に加入している視聴者は、容易に番組を視聴することができる。このような暗号化構成の帯域幅使用量(bandwidth cost)は、暗号化を適用する周波数帯域に依存する。上述の具体例では、各番組についてデータの1/9の追加的ファ

クタ (extra factor) が伝送される。この具体例では、およそ 1 番組相当の帯域幅が使用されている。番組数を多くすると、番組毎に暗号化されるパケット数は減り、暗号化システムのセキュリティは若干劣化する。ランダム化された M 番目 N パケット暗号化方式と同様に、ランダムフレームを選択してもよい。ビデオフレームの場合、ランダムフレームを選択することにより、全てのフレームタイプがアフェクトイントラ符号化フレーム (affected-intra-coded frame: I フレーム)、前方予測符号化フレーム (predictive-coded frame: P フレーム)、両方向予測符号化フレーム (bi-directional-coded frame: B フレーム) 及び DC フレームであることを保証する。

【 0 0 6 7 】

本発明の変形例において、暗号化するパケットの数を更に減らしても、許容範囲のセキュリティレベルを達成できる。すなわち、例えば 9 番組方式においては、1 秒間に 1 つのフレームを暗号化するだけで、許容範囲のセキュリティレベルを達成できる。このような方式では、オーバーヘッドは、1 番組につき 1 秒間に 1 暗号化期間となり、すなわち、オーバーヘッドにおいて約 $1/30$ のデータが伝送される。このようなオーバーヘッドの削減は、2 つの暗号化方式によるフルデュアルキャリッジに対応した帯域幅の 50% の伝送損失に比べると、著しい改善であると言える。本発明の他の変形例として、任意のビデオフレームのみを暗号化しても、許容範囲のセキュリティレベルを達成できる。例えば、MPEG コンテンツについて、I フレームだけをスクランブルすることにより、許容範囲のセキュリティレベルを維持したまま、帯域幅のオーバーヘッドを更に減少させることができる。これにより、フルデュアルキャリッジに必要な帯域幅を著しく削減することができる。

【 0 0 6 8 】

重要なパケットの暗号化

選択的なパケット毎のデュアル暗号化技術を用いることにより、帯域幅使用効率を大幅に高めることができる。このデュアル暗号化技術では、適切な番組コンテンツのオーディオ及び/又はビデオデータに対する重要性に基づき、暗号化するパケットを選択する。

【 0 0 6 9 】

この実施例では、パケットの小さな部分のみをスクランブルすることによって、暗号化コンテンツのフルデュアルキャリッジに比べ、帯域幅使用量を減少させることができる。クリアなパケットは、2 個以上のデュアルキャリッジ PID 間で共有される。好ましい一実施例において、後述するように、コンテンツ帯域幅全体の約 1% 未満を使用する。旧暗号化方式のシステムにおいて、暗号化していない番組コンテンツパケットは、旧型及び新型の両方のセットトップボックスによって受信することができる。上述のように、暗号化パケットは、二重に伝送され (dual carried)、それぞれのセットトップボックスによって適切な CA 方式で処理される。各 CA 方式は、直交している。各 CA 方式において、鍵の共有は不要であり、新旧異なる鍵が用いられていてもよい。例えば、モトローラ社所有の暗号化方式は、組込みセキュリティ ASIC によって高速変更暗号鍵 (fast changing encryption keys) を発生させることができ、一方、NDS 社のスマートカードベースのシステムでは、それより僅かに遅い変更暗号鍵を生成する。この実施例は、サイエンティフィックアトランタ社及びモトローラ社の旧式の暗号化方式に対しても同等にうまく動作する。

【 0 0 7 0 】

図 6 は、本発明の一実施例として、番組の一部をパケット毎にデュアル暗号化するシステム 300 のブロック図を示している。このシステム 300 において、各番組のパケットは、例えば旧式の CA 方式 A と新たな CA 方式 B を用いてデュアル暗号化される。暗号化されるパケットは、その重要度を基準に選択され、ビデオ及び/オーディオストリームの適切なデコーダに送られる。

【 0 0 7 1 】

図 6 に示すシステム 300 では、ケーブルシステムのヘッドエンド 322 は、パケット選択器 316 において A/V コンテンツ 304 の暗号化されるパケットを選択する。暗号化されるパケットは、それらが (料金未払いのデコーダによって) 受信不能であることが

、番組の実時間復号及び記録されたコンテンツのあらゆるポストプロセッシングに対して大きく影響するように選択される。すなわち、重要な(critical)パケット(以下、クリティカルパケットという。)のみが暗号化される。ビデオパケット及びオーディオパケットに対して、クリティカルパケットの暗号化は、PES(パケット化エレメンタリストリーム(packetized elementary stream))ヘッダ及びペイロードの一部としての他のヘッダを含む「フレーム開始(start of frame)」トランスポートストリームパケットを暗号化することにより達成することができる。これらの情報がなければ、STBのデコーダは、MPEG圧縮データを伸張することができない。MPEG2ストリームは、トランスポートヘッダ内の「パケット単位開始インジケータ(packet Unit Start Indicator)」によって「フレーム開始」パケットを識別する。一般的に、GOPヘッダ又はビデオシーケンスヘッダを含むペイロードを伝送するパケットを用いることによって、このスクランブル技術を実現することができる。

【0072】

MPEG(Moving Pictures Expert Group)方式に準拠した圧縮ビデオデータは、エレメンタリデータストリームを188バイトのデータを含むある程度(somewhat)任意のペイロードのトランスポートストリームに再パッケージ化する。このように、PESヘッダを含むトランスポートストリームパケットは、パケット選択器316において暗号化されるものとして選択され、CA方式A暗号化器318とCA方式B暗号化器324の両方によってデュアル暗号化される。デュアル部分暗号化されるパケットは、複製され、暗号化器324によって暗号化され、複製されたパケットのPIDは、上述の実施例と同様に、第2のPID割当器330において第2のPIDに割り当てられる。残りのパケットは、クリアなまま渡される。クリアなパケットと、CA方式Aによって暗号化されたパケットと、CA方式Bによって暗号化されたパケットと、システム情報328と、PSI329とは、互いに多重化され、ケーブルシステム32を介して放送される。

【0073】

上述した方式と同様に、旧型のSTB36は、クリアなデータ及びCA方式Aによって暗号化されたデータを受信し、CA方式A40によって復号されたデータと暗号化されていないデータを組み合わせてトランスペアレントにSTB36のデコーダに供給する。新型のSTB336において、番組は、第1のPID及び第2のPIDの両方に割り当てられている。第1のPIDを有するクリアなパケットは、受信されてデコーダに供給される。第1のPIDを有する暗号化されたパケットは、除外(discarded)される。第2のPIDを有する暗号化されたパケットは、復号されて、デコードのために、(例えば、パケットを第1のPIDに再マッピングすることによって)データストリームに再挿入される。

【0074】

ビデオデータを具体例として説明すると、各サンプルは、フレームと呼ばれ、サンプリングレートは、通常、30フレーム毎秒である。3.8Mbpsに適合するようにサンプルを符号化する場合、各フレームは、帯域幅のうちの127kビットを占有する。MPEGトランスポートのデータは、188バイトのパケットに分割(sliced)され、各フレームの第1のパケットは、フレームデータの本体の処理を指示するために用いられるヘッダを含んでいる。第1のヘッダパケットのみ(追加的な1504ビット)をデュアル暗号化する場合、必要となる追加的な帯域幅は、1.2%(1504/127k)のみである。高精細度(high definition)ストリーム(19Mbps)の場合、この割合は更に小さくなる。

【0075】

上述のように、本発明の実施例においては、PESヘッダを含むトランスポートストリームパケットを暗号化の対象とすることが望ましい。これらのパケットは、シーケンスヘッダ(sequence header)と、シーケンス拡張ヘッダ(sequence extension header)と、ピクチャヘッダと、同じパケット内にも含まれる量子化及び他のデコードテーブルとを含んでいる。これらのパケットをデコードできない場合、(すなわち、ハッカーが加入料を

払わないで、許可されていない番組を視聴しようとした場合)、番組の大部分が視聴できない。多くの場合、番組を選局しようとしても、ブランク画面が表示されるだけであり、周知のデコーダ集積回路は、PESヘッダを用いて、ビデオ及びオーディオ等のエレメンタリストリームを実時間で同期させているため、音声も聞こえない。PESヘッダを暗号化することにより、未許可のセットトップボックス内のデコードエンジンは、動作を開始することすらできない。例えば保存されたコンテンツに対するポストプロセッシング攻撃(post processing attacks)は、PESヘッダを含むパケット内の動的に変化する情報によって防がれる。本発明の主旨から逸脱することなく、未許可の視聴を防止するために、この他のクリティカルな、すなわち重要なパケット、又はコンテンツ要素を暗号化してもよいことは当業者にとって明らかである。例えば、MPEGイントラ符号化フレーム、すなわちIフレームピクチャパケットを暗号化して、番組のビデオ部分の視聴を制限してもよい。本発明のこの実施例は、他の如何なる実施例と組み合わせてもよく、例えば、PESヘッダを含むパケットを暗号化するとともに、他のパケットに対してランダム暗号化、M番目N暗号化、又はデータ構造暗号化を施してもよい。クリティカルパケット暗号化を用いてビデオデータを暗号化し、他の暗号化方式をオーディオデータに適用してもよい。オーディオデータは、例えば、デュアル暗号化してもよい。当業者は、本発明の範囲内で様々な変形例を想到することができる。

【0076】

図7は、例えば図6に示すヘッドエンド322に適用される具体的な符号化処理を説明するフローチャートである。トランスポートストリームパケットを受信すると、ステップ350において、パケットを調べ、このパケットが暗号化のための選択基準(selection criteria)を満たすか否かを判定する。好ましい実施例においては、選択基準は、パケットペイロードの一部としてPESヘッダが存在していることである。この選択基準を満たさない場合、パケットは、クリアな、暗号化されていないパケット(C)として渡され、ステップ354において、出力データストリームに挿入する。パケットがこの選択基準を満たす場合、ステップ358において、このパケットをCA暗号化方式Aで暗号化し、暗号化されたパケットEAを生成する。更に、このパケットを複製し、ステップ362において、複製されたパケットをCA暗号化方式Bで暗号化し、暗号化されたパケットを生成する。ステップ366において、この暗号化されたパケットを第2のPIDにマッピングし、これにより、暗号化されたパケットEBを生成する。ステップ354においては、暗号化されたパケットEA、EBをクリアなパケットCとともに、出力データストリームに挿入する。好ましくは、暗号化されたパケットEA、EBは、データストリームにおいて、元の単一のパケットが暗号化のために取り出された位置に挿入し、データのシーケンスが基本的に同じになるようにするとよい。

【0077】

ステップ354において生成された出力データストリームが、例えば図6に示すSTB336等のCA暗号化方式Bに準拠したSTBによって受信されると、図8(図5に類似している。)に示すような処理により、番組を復号及びデコードする。第1のPID又は第2のPIDを有するパケットが受信されると、ステップ370において、パケットがクリア(C)であるか、CA暗号化方式Aに基づいて暗号化されているか(EA)を判定し、ステップ374において、このパケットがCA暗号化方式Bに基づいて暗号化されているか(EB)を判定する。パケットがクリアである場合、このパケットをデコーダ378に直接渡す。幾つかの実施例においては、第1(第2)のパケットが第2(第1)のパケットの前にあるか又は後ろにあるかといった相対的位置に基づいて、第1(第2)のパケットをストリーム内で検出してもよい。この場合、第1のパケットのスクランブル状態を特に確認する必要はない。パケットがEAパケットである場合、ステップ380において、このパケットを破棄する。パケットEBパケットである場合、ステップ384において、このパケットを復号する。この時点において、ステップ388において、第2のPIDパケット及び/又は第1のPIDパケットを同じPIDに再マッピングする。そして、デコーダ378において、復号されたパケット及びクリアなパケットをデコードする。

【 0 0 7 8 】

上述したデュアル部分暗号化方式によって、フルデュアルキャリアッジの場合に比べて、帯域幅要求を大幅に削減することができる。P E S ヘッダ情報の暗号化は、ビデオ及びオーディオコンテンツの安全性を確保する点で有効であるとともに、これにより、同じケーブルシステム内に2つ以上のC A方式を独立して「共存 (co-exist)」させることができる。この場合、旧型のA方式のセットトップボックスには影響がなく、B方式のセットトップボックスも、ビデオ及びオーディオデータについて2つのP I Dを参照するよう、ハードウェア、ファームウェア又はソフトウェアを僅かに拡張すればよい。旧型及び非旧型のS T Bは、それぞれの基本的なC A方式を維持する。ヘッドエンドの変更は、暗号化するためのコンテンツを選択する点のみに限られ、すなわち、第2の暗号化器と、暗号化されたパケットと暗号化されていないパケットとを混合して合成出力ストリーム (composite output stream) を生成する回路とを設ければよい。

【 0 0 7 9 】

一実施例においては、ヘッドエンド装置は、状況に応じて、クリティカルなP E S ヘッダのみではなく、帯域幅が許す限り多くのコンテンツを暗号化する。これらの更なる暗号化されたパケットは、P E S ペイロード内のパケットであっても、ビデオ/オーディオフレームにおける他のパケットであってもよく、これにより、コンテンツの安全性が更に高められる。

【 0 0 8 0 】

S I 暗号化 (S I ENCRYPTION)

図9は、更なる帯域幅の必要性を最小化するシステム400の具体的構成を示している。この実施例では、システム400は、セットトップボックスにおいて、番組を選局するためには、システム情報 (S I) 428が必要であるという事実を利用している。ケーブルシステムでは、S Iは、帯域外 (out-of-band)、すなわち通常の視聴チャンネルの周波数以外の周波数で伝送される。また、S Iは、帯域内 (in-band) で送信してもよい。帯域内で送信する場合、S I 428は、各ストリームに対して複製され、各ストリームとともに送信される。説明のために、「旧型の」セットトップボックスに供給されるS Iが、例えばS T B 436等の新しいセットトップボックスに供給されるS Iとが分離されているとする。これにより、S I 428の各バージョンは、C A方式A 418とC A方式B 424を用いて個別に暗号化される。クリアなビデオデータ404及びクリアなオーディオデータ406は、クリアな形式で配信されるが、これがクリアであることを示すためには、S I 428が必要である。

【 0 0 8 1 】

S Iは、チャンネル名、及び例えばプログラム名、開始時刻等を含むプログラム案内情報等の情報とともに、各チャンネルの周波数選局情報 (frequency tuning information) を含んでいる。デジタルチャンネルは、互いに多重化され、特定の周波数を介して伝送される。本発明の実施例では、S I情報は暗号化され、許可されたセットトップボックスのみで利用可能となる。システム (plant) 内の全てのA / V周波数の割り当てを示すS I情報が受信されなかった場合、選局を行うことはできない。

【 0 0 8 2 】

セットトップボックスを改造して、周波数の試行又はスキヤニングを行おうとするハッキング行為を不能にするために、チャンネルの周波数を、標準的な周波数からオフセットさせてもよい。更に、日毎、週毎又はこの他の周期で、若しくはランダムに、周波数を動的に変更してもよい。一般的なケーブルシステムのヘッドエンドは、約30個の周波数帯域を用いる。各周波数は、多くの場合、相互の周波数間で、地上波放送信号との間で、及び受信装置のクロックとして用いられている周波数との間で干渉が生じないように、選択される。各チャンネルは、使用されても干渉を生じず、若しくは使用されると隣接するチャンネルの周波数が変更される独立した少なくとも1つの代替周波数 (alternate frequency) を有する。したがって、実際に可能な周波数マップは、230又は107 × 109個となる。ここで、ハッカーは、単純に、各局の両方の周波数について、30個のチャン

ネルのそれぞれを試すような行為を行う可能性もある。コンテンツを提供する周波数の特定に成功すると、ハッカーのセットトップボックスは、P S I 4 2 9を解析し、番組を構成する個々のP I Dに関する情報を得る。ここで、ハッカーが「番組1」が「C N N」の番組であり、「番組5」が「T N N」の番組である、といったことを特定することは困難である。このような情報は、上述のように暗号化され、未許可のセットトップボックスでは利用できないS Iとともに送信されている。しかしながら、ハッカーが配信されたコンテンツのそれぞれを選択し、調べれば、番組と局の対応関係も把握することができる。このようなチャンネルの特定を妨害するために、単一のストリーム内の番組の割り当てを時刻によって変更し、例えば、上述した具体例における番組1と番組5とを入れ替え、「番組1」を「T N N」にし、「番組5」を「C N N」にするなどして、ハッカーを混乱させてもよい。或いは、全く新しい番組のグループ化に基づいて、番組を全く異なるストリームに移動させてもよい。一般的なケーブルシステムのヘッドエンドは、音楽番組を含む250個の番組のコンテンツを配信する能力を有する。それぞれの番組を固有に選局することができる。再順序付けの可能な組合せは250! (階乗)個である。配信されたS I又はハッカーのいずれかによって提供されたコンテンツのマップがなければ、ユーザは、番組をランダムに選局して、その番組に興味があるものであるか否かを確認めなくてはなくなる。

【0083】

このように、ヘッドエンド422においては、ビデオ信号404及びオーディオ信号406がクリアな(暗号化されていない)形式で供給され、S I 428は、複数のC A方式に基づき、ケーブルネットワークを介して配信される。したがって、この具体例に示すシステム400においては、クリアなS I 428は、暗号化器418に供給され、暗号化器418は、暗号化方式Aを用いてS I 428を暗号化する。同時に、クリアなS I 428は、暗号化器424にも供給され、暗号化器424は、暗号化方式Bを用いて、S I 428を暗号化する。次に、クリアなビデオ信号404、オーディオ信号406及びP S I 429は、暗号化器418からの暗号化されたS I (S I A)、暗号化器424からの暗号化されたS I (S I B)とともに多重化され、帯域外システム情報428を置換する。

【0084】

ケーブルシステム32を介して配信された後、ビデオデータ、オーディオデータ、システム情報A、システム情報Bは、全て、セットトップボックス36及びセットトップボックス436に供給される。S T B 36においては、暗号化されたS Iは、C A方式A40において復号され、セットトップボックスに選局情報が提供される。セットトップボックス36は、特定の番組を選局し、テレビジョン受信機44に表示させる。同様に、S T B 436においては、暗号化されたS Iは、C A方式B440において復号され、セットトップボックスに選局情報が提供され、これにより、特定の番組を選局し、テレビジョン受信機444に表示できるようになる。

【0085】

この手法により、例えばケーブルシステム等のコンテンツ配信システムにおいて、追加的なA/V帯域を用意する必要がなくなるという利点がある。ここでは、S Iのみがデュアル伝送(dual carried)される。特別なハードウェアも不要である。大部分のチューナは、標準周波数からの如何なるオフセット周波数にも容易に適応することができる。S I復号は、ソフトウェアによって実行してもよく、ハードウェアの助けを借りて行ってもよい。例えば、旧型のモトローラ社(Motorola)のセットトップボックスは、デコーダ集積回路チップ内に組み込まれたハードウェア復号器を用いて、帯域外周波数帯を介してモトローラ社のセットトップボックスに配信されたS Iを復号する能力を有する。

【0086】

ハッカーが同軸ケーブルにスペクトルアナライザを用いて、A/Vチャンネルを特定する可能性もある。更に、比較的時間がかかる処理であるが、ハッカーがセットトップボックスを改造して、周波数帯域を自動スキャンし、A/Vチャンネルを特定する可能性

もある。A/Vチャンネル周波数を動的に変化させれば、ハッカーは、継続的に帯域を分析又はスキャンしなくてはならなくなり、このようなハッカーの行為を挫折させることができる。更に、プログラム番号及び割り当てられるPIDを変更してもよい。但し、周波数、プログラム番号、PIDを動的に変更すると、例えば、ケーブルシステムのオペレータ等のサービスプロバイダにおける処理が複雑になる。

【0087】

包括的表現 (GENERALIZED REPRESENTATION)

上述した各手法は、包括的に、図10のシステム500として表現することができる。このシステム500は、ケーブルシステムヘッドエンド522を備え、ケーブルシステムヘッドエンド522は、クリアなビデオデータ504と、クリアなオーディオデータ506と、SI528と、PSI529とを備え、これらは、インテリジェントプロセッサによって制御されたスイッチ518を介して選択的に切り換えられ、スイッチ518は、PIDの割当 (PID割当又は再割当を要求する実施例において) を行い、上述した各データを選択的に、CA方式A520又はCA方式B524に供給し、或いは、クリアな形式でケーブルシステム32に供給する。従来と同様、旧式のCA方式Aによって暗号化された番組又はSIは、STB36によって正しく復号される。CA方式Bによって暗号化された情報は、上述のように、STB536によって検出され、復号され、デコードされる。

【0088】

PIDマッピングに関する考察

上述したPIDマッピングの概念は、必要に応じて、ここに説明したデュアル部分暗号化方式に適用することができる。包括的には、ケーブルシステムのヘッドエンドにおいて、パケットのデータストリームは、暗号化のために選択されたパケットを複製するように操作される。これらのパケットは、複製され、2つの異なる暗号化方式に基づいて暗号化される。複製されたパケットには、個別のPID (これらのうちの1つは、クリアなコンテンツに用いられる旧型のCAのPIDに対応する) が割り当てられ、これらのパケットは、データストリームにおける元の選択されたパケットの位置に挿入され、ケーブルシステムを介して伝送される。ケーブルシステムのヘッドエンドからは、同じPIDを有する旧式の暗号化が施されたパケット及びクリアなパケットのストリームが出力される。第2のPIDは、パケットが新しい暗号化方式で暗号化されていることを示す。ヘッドエンドで行われるPID再マッピングに加えて、MP EGパケットは、連続カウンタ (continuity counter) を利用して、パケットの適切なシーケンスを維持する。適切な復号が行われることを保証するために、ヘッドエンドにおいて、パケット化されたデータストリームを生成する間、この連続カウンタを適切に維持する必要がある。これは、各PIDを有するパケットが、連続カウンタに通常の手法で連続的に割り当てられるようにすることで達成される。これにより、第2のPIDを有するパケットは、第1のPIDの連続カウンタからは、独立した連続カウンタを有することとなる。これを単純な形式で以下に示す。ここでは、PID025は、第1のPIDであり、PID125は、第2のPIDであり、Eは、暗号化されたパケットを表し、Cは、クリアなパケットを表し、末尾の数字は、連続カウンタを表す。

【0089】

【表9】

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12
--------	--------	--------	--------	--------	--------	--------	--------	--------

【0090】

この例示的なパケットのセグメントでは、PID025を有するパケットは、独自の連続カウンタのシーケンス (04, 05, 06, 07, 08, 09, ...) を有する。同様に、第2のPID125を有するパケットは、独自の連続カウンタのシーケンス (11, 12, ...) を有する。STBにおいては、PIDは、任意の数の手法で処理するこ

とができ、第2のPIDを有する暗号化されたパケットと正しい番組とが適切に関連付けられる。パケットヘッダを含む入力ストリームセグメントの一具体例を以下に示す。

【0091】

【表10】

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12
--------	--------	--------	--------	--------	--------	--------	--------	--------

【0092】

この入力ストリームを処理することにより、次のような出力ストリームセグメントが生成される。

【0093】

【表11】

125C04	025E11	125E05	125C06	125C07	125C08	125C09	025E12	125E10
--------	--------	--------	--------	--------	--------	--------	--------	--------

【0094】

第1のPID(025)は、入力ストリーム内のクリアなパケット(C)用の第2のPID(125)に置換される。暗号化されたパケットについては、第1のPID及び第2のPIDが維持されるが、連続カウンタが入れ替えられる。これにより、パケットのストリームは、第2のPIDを用いることによる継続性の喪失によるエラーを生じることなく正しく復号及びデコードできる。本発明の実施例とともに、PIDの処理に関する他の手法として、例えば、スクラビングされた旧型のパケットのPID(125)をNOP PID(全てが1)又は復号されない他のPID値にマッピングしてもよく、連続カウンタを用いてもよい。

【0095】

第1及び第2のPIDは、番組特定情報(program specific information: PSI)データストリームの一部として伝送される放送番組マップテーブル(program map table: PMT)に含まれてSTBに供給される。第2のPIDの存在は、CA暗号化方式A(「旧式の」方式)に基づいて動作するSTBによっては無視することができ、一方、CA暗号化方式Bに基づいて動作する新たなSTBは、第2のPIDが第1のPIDに関連する番組の暗号化された部分を伝送するために用いられていることを認識するようプログラミングされる。セットトップボックスには、PMTの基本PID「フォールブ(for loop)」におけるCA記述子の存在によって、暗号化方式が用いられていることが知らされる。通常、ビデオ基本PID「フォールブ」のためのCA記述子と、オーディオ基本PID「フォールブ」のための他のCA記述子とが存在する。CA記述子(CA descriptor)は、プライベートデータバイト(Private Data Byte)を用いて、CA_PIDをECM PID又は部分暗号化に用いる第2のPIDとして識別し、これにより、STBの動作を単一の番組に関連する第1及び第2のPIDを検出する方式Bに設定する。トランスポートヘッダ内のPIDフィールドは、13ビット長であるため、213すなわち8192個のPIDを使用することができ、必要に応じて、予備の如何なるPIDを第2のPIDとして用いてもよい。

【0096】

各番組コンポーネントに又は番組コンポーネントの選択された部分にPIDを割り当てることに加えて、第2の暗号化方式において用いるタグECMデータに新たなPIDを割り当ててもよい。割り当てられる各PID番号は、旧型のSTBの動作に支障を生じさせないために、ユーザにより定義されたストリームタイプとして指定される。MP EGでは、このような数の予備ブロックを、ユーザにより定義されたデータストリームタイプとして定義している。

【0097】

ケーブルヘッドエンドにおけるPIDマッピングは、概念的にも、単純な処理であり、

実際に、ケーブルヘッドエンドの設備は、既にこのようなマッピングに対応しており、したがって、既存のケーブルシステムの最小限の変更で、低コストに、このような方式を実現することができる。ケーブルシステムヘッドエンド内において、この方式をどのように実現するかについては、後に具体例を挙げて詳細に説明するように、ヘッドエンド内の実際の旧型のハードウェアに依存する。

【0098】

ヘッドエンドの実現

図2、図3、図6、図9、図10を参照して説明した上述の実施例は、ある程度概念的な性質を有し、本発明の様々な実施例に関連する全体的な発想及び概念を説明するために用いられていることは、当業者にとって明らかである。本発明を現実的に実現するためには、既に設立されているケーブルプロバイダの既存の旧型のヘッドエンド装置において、様々な部分暗号化方式について、コスト効率が高い実現が必要であるという現実世界での重要な問題があることは当業者にとって明らかである。ここでは、2つの旧型のケーブルシステムを具体例として、上述の手法をケーブルヘッドエンドにおいてどのように実現するかを説明する。

【0099】

まず、モトローラ社の限定受信技術を用いたケーブルシステムヘッドエンドについて考察する。このようなシステムでは、デュアル部分暗号化を低コストで実現するために、図11に示すような変更を行うことができる。典型的なモトローラ方式であるヘッドエンドインザスカイ(Headend In The Sky: 以下、HITSという。)又は類似の方式では、信号は、衛星から供給される。この方式では、ケーブルプロバイダから提供され、例えば、モトローラ集積受信機トランスコーダ(Motorola Integrated Receiver Transcoder: IRT)モデルIRT1000及びIRT2000及びモトローラモジュラ処理システム(Motorola Modular Processing System: MPT)等の受信機/デスクランブラ/スクランブラシステム604に受信される集合的な(aggregated)デジタル化されたコンテンツを提供する。デジタルテレビジョンデータのクリアなストリームは、受信機/デスクランブラ/スクランブラシステム604の衛星デスクランブラ機能ブロック606から得ることができる。このクリアなストリームは、パケット選択器/デュプリケータ610として示す新たな機能ブロックによって処理される。このパケット選択器/デュプリケータ610は、プログラミングされたプロセッサとして、又はハードウェア又はソフトウェア及びこれらの組合せとして実現できる。

【0100】

パケット選択器/デュプリケータ610は、上述したデュアル部分暗号化のうちのいずれかに基づいてデュアル暗号化すべきパケットを選択する。これらのパケットは、複製され、後の暗号化において特定できるように、新たなPIDが付される。例えば、パケット選択器/デュプリケータ610に供給された特定の番組に関連するパケットがPID「A」を有する場合、パケット選択器/デュプリケータ610は、そのパケットを暗号化すべきパケットであると識別し、これらのパケットを複製し、これらのパケットにPID「B」、PID「C」をそれぞれ再マッピングする。これにより、後の暗号化において、これらのパケットを異なる2つの方式に応じて特定することができる。好ましくは、複製されたパケットは、PID「B」、PID「C」とともに、互いに隣接して、データストリームの複製された元のパケットの位置に挿入される。これにより、これらのパケットは、元の位置を維持する(但し、元のデータストリームには1つのパケットしかなかった位置に2つのパケットが存在することとなる)。ここで、追加すべき新たなCA方式がNDS方式の暗号化であるとする。この場合、PID「A」は、クリアなパケットを表し、PID「B」は、NDS方式で暗号化されたパケットを表し、PID「C」は、モトローラ方式で暗号化されたパケットを表す。PID「B」を有するパケットは、この時点で、パケット選択器/デュプリケータ610において、NDS暗号化方式で暗号化してもよく、後に暗号化してもよい。

【0101】

P I D 「 B 」 及び P I D 「 C 」 を有するパケットは、受信機 / デスクランブラ / スクランブラシステム 6 0 4 に戻され、ここで、P I D 「 C 」 を有するパケットは、モトローラの装置に関連する制御方式 6 1 4 に基づき、ケーブルスクランブラ 6 1 2 において、モトローラ暗号化方式で暗号化される。ケーブルスクランブラ 6 1 2 からの出力ストリームは、更なる新たな装置である P I D 再マッピング及びスクランブラ 6 2 0 に供給され、P I D 再マッピング及びスクランブラ 6 2 0 は、ケーブルスクランブラ 6 1 2 から受け取ったデータについて、残りのパケットに P I D 「 A 」 乃至 P I D 「 C 」 を再マッピングし、制御方式 6 2 4 による制御に基づき、N D S 暗号化アルゴリズムを用いて、P I D 「 B 」 を有するパケットを暗号化する。出力ストリーム 6 2 6 は、P I D 「 C 」 を有するクリアな暗号化されていないパケットと、複製され、選択され、モトローラ暗号化方式によって暗号化された P I D 「 C 」 を有するパケットと、複製され、選択され、N D S 暗号化方式によって暗号化された P I D 「 B 」 を有するパケットとを含む。このストリームは、ケーブルシステムを介して配信するために、変調器 6 2 8 (例えば、直交振幅変調 (quadrature amplitude modulation : 以下、Q A M という。) 又は R F 変調により) で変調される。好ましい実施例では、旧型の番組特定情報 (P S I) において用いられているオーディオ及びビデオ P I D との互換性を保つために、P I D 「 A 」 が付された暗号化されていないパケットを P I D 「 C 」 が付されたスクランブルされたパケットに一致するようにマッピングする。制御コンピュータ、スクランブラ及び旧型のセットトップボックスは、P I D 「 C 」 に関する知識のみを有している。これに代えて、P I D 「 C 」 が付されたスクランブルされたパケットを逆に P I D 「 A 」 にマッピングしてもよいが、この場合、自動的に生成された P S I を編集して、P I D 再マッピング及びスクランブラ 6 2 0 において P I D 「 C 」 からの P I D 番号を P I D 「 A 」 に振り直す必要がある。

【 0 1 0 2 】

上述の実施例において、P I D 再マッピング及びスクランブラ 6 2 0 は、P S I 情報の複製に用いることもでき、この場合、P I D 再マッピング及びスクランブラ 6 2 0 は、P S I 情報を変更して、(P M T における C A 記述を用いて) N D S 暗号化の追加を反映させ、変更した P S I 情報をデータストリームに多重化して戻してもよい。更に、P I D 再マッピング及びスクランブラ 6 2 0 において、N D S 暗号化をサポートする E C M をデータストリームに挿入してもよい (又は、パケット選択器 / デュプリケータ 6 1 0 によってこれを挿入してもよい) 。

【 0 1 0 3 】

このように、N D S 暗号化方式 (又は、この他の暗号化方式) をモトローラ社の設備を用いるケーブルシステムヘッドエンドに追加するために、パケットが複製され、衛星デスクランブラからのデータストリームにおいて P I D が再マッピングされる。再マッピングされた P I D は、各 C A 方式に基づいてスクランブルすべきパケットを特定するために用いられる。旧式の暗号化方式を採用する場合、クリアなパケットの P I D は、旧式の方式におけるクリアなパケットと暗号化されたパケットの両方が同じ P I D (又は複数の P I D) を共有するように再マッピングされる。P I D 再マッピング及びスクランブラ 6 2 0 における P I D の再マッピング及びパケット選択器 / デュプリケータ 6 1 0 におけるパケットの選択と複製は、プログラミングされたプロセッサ、若しくは、例えば特定用途向け集積回路等のカスタムの又はセミカスタムの集積回路、プログラマブルロジックデバイス又はフィールドプログラマブルゲートアレーを用いて実現してもよい。本発明の範囲から逸脱することなく、これらを別の手法で実現することもできる。

【 0 1 0 4 】

図 1 2 は、サイエンティフィックアトランタ社のケーブルヘッドエンドにおいて、本発明に基づくデュアル部分暗号化を実現するために用いる同様の設備構成を示している。この実施例では、H I T S 信号又は同様の信号が衛星信号デスクランブラ 7 0 6 が組み込まれた I R D 7 0 4 において受信される。これは、衛星信号デスクランブラ機能がイネーブルにされたモトローラ社の I R T 又は M P S であってもよい。衛星信号デスクランブラ 7 0 6 からの出力信号は、新たなパケット選択器 / デュプリケータ 7 1 0 によって処理でき

るクリアなデータストリームであり、パケット選択器/デuplicータ710は、パケット暗号化すべきパケットを選択し、これらを複製し、複製されたパケットのPIDを新たなPIDにマッピングする。ここでも、例えば、クリアなまま残すパケットには、PID「A」が割り当てられ、新たな方式(例えば、NDS)で暗号化すべきパケットには、PID「B」が割り当てられ、サイエンティフィックアトランタ社の方式で暗号化すべきパケットには、PID「C」が割り当てられる。パケットPID「B」が付されたパケットは、この時点で、NDS暗号化方式で暗号化される。

【0105】

パケットのストリームは、マルチプレクサ712(例えば、サイエンティフィックアトランタ社製マルチプレクサ)に供給され、マルチプレクサ712は、マルチプレクサ712に関連する制御方式718による制御の下、ケーブルスクランブラ714において、PID「C」を有するパケットをサイエンティフィックアトランタ暗号化方式で暗号化する。次に、データストリームは、マルチプレクサ712の内部でQAM変調器720に供給される。パケットを正しく再マッピングするために、マルチプレクサ712から出力されるQAM変調信号は、新たな処理部724に供給され、ここで、QAM変調信号は、QAM復調器730によって復調され、次に、PID再マッピング器734において、制御方式738による制御の下、クリアなPID「A」パケットがPID「C」に再マッピングされる。NDS暗号化アルゴリズムに基づく暗号化もパケット選択器/デuplicータ710ではなく、ここで実行される。PIDが再マッピングされ、デュアル部分暗号化されたデータストリームは、QAM及びRF変調器742によってQAM変調及び/又はRF変調された後、ケーブルシステムを介して配信される。

【0106】

上述の実施例においては、更に、PID再マッピング及びスクランブラ734を用いて、PSI情報の逆多重化し、PSI情報にNDS暗号化の付加を反映させ(PMTにCA記述子を追加する)、変更されたPSI情報をデータストリームに戻す。PID再マッピング及びスクランブラ734において、データストリームにNDS暗号化をサポートするためのECMを挿入してもよい(或いは、これをパケット選択器/デuplicータ710によって挿入してもよい)。PID再マッピング及びスクランブラ734におけるPID再マッピング及び/又はスクランブル、QAM復調器730及びQAM及びRF変調器742によるQAM復調及びQAM変調、及びパケット選択器/デuplicータ710におけるパケットの選択と複製は、プログラミングされたプロセッサ、若しくは、例えば特定用途向け集積回路等のカスタムの又はセミカスタムの集積回路、プログラマブルロジックデバイス又はフィールドプログラマブルゲートアレーを用いて実現してもよい。本発明の範囲から逸脱することなく、これらを別の手法で実現することもできる。

【0107】

本発明の上述の実施例により、旧型のスクランブル装置は、全てのエレメンタリストリームではなくエレメンタリストリームにおける望まれるパケットのみをスクランブルできる。任意のパケットの選択的なスクランブルは、エレメンタリストリームにおけるスクランブルする必要がないパケットに対し、例えば、PID「A」といった所定のPID番号を付すことによって実現する。スクランブルされるパケットには、例えば、PID「C」を付す。スクランブル装置は、PID「C」が付された(スクランブルすると選択された)パケットをスクランブルする。スクランブルが行われた後、スクランブルされていないパケットは、スクランブルされたパケットにマッピングされたPID番号と同じPID番号を有することとなり、PID「A」がPID「C」となる。旧型のセットトップボックスは、スクランブルされたパケット及びスクランブルされていないパケットの両方とともにエレメンタリストリームを受信する。

【0108】

これらの実施例におけるパケットは、ストリームとして処理される。全体のストリームは、スクランブルのために旧型のスクランブル装置に供給される。これにより、全てのパケットが正確な時間同期順に保たれる。パケットがストリームから抽出され、旧型のスク

ランブル装置に供給されると、時間的ジッタ (time jitter) が導入されることがある。この実施例では、ストリーム内に全てのパケットを維持することによって、この問題を回避している。この実施例では、旧型のスクランブル装置は、パケットの再マッピングの処理、すなわちパケット P I D 「 A 」から P I D 「 C 」への再マッピング処理に参加しないため、旧型のスクランブル装置の製造業者による協力を必要としない。この再マッピングでは、旧型のスクランブル装置によって生成される P S I によって処理される P I D 「 C 」を変更する必要がないという利点がある。旧型のシステムは、P I D 「 C 」に関する知識を有するが、P I D 「 A 」に関する知識は有さない。旧型のスクランブル装置によってスクランブルすべき全体的なエレメンタリストリームは、スクランブルシステムがスクランブルするように指示されている単一の P I D によって示される。

【 0 1 0 9 】

上述の実施例において、第 2 の暗号化方式として用いる N D S は、例示的なものであり、本発明を限定するものではない。更に、広く用いられている 2 つの方式、すなわち、モトローラ社及びサイエンティフィックアトランタ社の方式を例示的に説明したが、他の旧型のシステムを同様に変更して P I D 再マッピング及びデュアル部分暗号化を実現することもできる。包括的には、上述した技術は、図 1 3 に包括的に示す処理 8 0 0 を含む。ステップ 8 0 6 においては、フィード (feed) を受信し、ステップ 8 1 0 において、このフィードをデスクランブルして、クリアなパケットのデータストリームを生成する。ステップ 8 1 4 において、所望のデュアル部分暗号化方式 (例えば、オーディオのみ、P E S ヘッダを含むパケット等) に応じてパケットを選択する。ステップ 8 1 8 において、選択されたパケットを複製し、複製された対を新たな 2 つの P I D (例えば、P I D 「 B 」及び P I D 「 C 」) に再マッピングする。ステップ 8 2 2 において、複製されたパケットを P I D に基づいて暗号化する (すなわち、P I D 「 C 」のパケットは、旧式の暗号化方式に基づいて暗号化し、P I D 「 B 」のパケットは、新たな暗号化方式に基づいて暗号化する)。ステップ 8 2 6 において、クリアなパケットの P I D (例えば、P I D 「 A 」) を旧式の方式で暗号化されたパケットの P I D (P I D 「 C 」) と同じ P I D に再マッピングする。

【 0 1 1 0 】

図 1 3 に示す処理 8 0 0 の各ステップの実行順序は、用いられるデュアル部分暗号化構成を含めるように変更される特定の旧型の方式に応じて、様々に変更してもよい。例えば、新たな暗号化方式に基づく暗号化は、複製を行う時点で行ってもよく、図 1 1 及び図 1 2 に示すように、後に旧式のパケットを再マッピングする際に、更に (図 1 3 には示さないが) 併用する特定の旧式の方式に対応するために、必要に応じて、様々な復調及び再変調処理を行ってもよい。

【 0 1 1 1 】

セットトップボックスの実現

本発明の範囲内において、様々なセットトップボックスの構成を用いることができる。ヘッドエンドにおいて、暗号化するためのパケットを選択する手法は、S T B には無関係である。

【 0 1 1 2 】

このような実現例の 1 つを図 1 4 に示す。この実施例では、チューナ及び復調器 9 0 4 からのパケットは、デコーダ回路 9 0 8 のデマルチプレクサ 9 1 0 に供給される。パケットは、(例えば、統合メモリアーキテクチャ (unified memory architecture) を用いて) メモリ 9 1 2 にバッファリングされ、R O M メモリ 9 2 0 に格納されているソフトウェアに基づいて動作する S T B のメイン C P U 9 1 6 によって処理される。

【 0 1 1 3 】

選択された P I D は、S T B の P I D フィルタによって、供給されてくるトランスポートストリームから抽出され、個人用ビデオレコーダ (Personal Video Recorder : P V R) アプリケーションにおけるハードディスクドライブ (Hard Disk Drive : H D D) への転送を準備するために必要な初期的な処理と同様に、復号され、同期ダイナミックランダ

ムアクセスメモリ (Synchronous Dynamic Random Access Memory : 以下、S D R A M という。) にバッファリングされる。ホスト C P U 9 1 6 は、「非自動で (manually)」 S D R A M にバッファリングされたデータをフィルタリングし、不必要な P I D を含むパケットを除外する。この処理には、幾つかの明らかな副次的作用 (obvious side effects) がある。

【 0 1 1 4 】

ホスト C P U のオーバヘッドは、C P U の帯域幅の約 1 % と推定される。最悪の場合、このオーバヘッドは、1 5 M ビット / 秒のビデオストリームにおける 4 0 k バイト / 秒に相当する。評価されるデータは、各パケットについて多くても 4 バイトのみであり、これらは、1 8 8 バイト分の間隔をあけて現れるので、間にあるデータは考慮しなくてもよく、このような削減が可能である。したがって、S D R A M 内の各パケットヘッダは、メモリポインタの簡単な操作によって、直接読み出すことができる。更に、パケットは、ブロックにキャッシュされ、まとめて評価されるため、ホスト C P U の切替タスクを軽減することができる。

【 0 1 1 5 】

これにより、新たな各パケットを受け取る毎に、他のタスクに割込が生じることを回避することができる。このような処理では、チャンネルの変更時に、キャッシュを満たすために必要な時間分、デコードの開始のための待ち時間が長くなる。このような待ち時間は、割り当てられる S D R A M キャッシュのバッファサイズによっては、無視することができる程度のものである。

【 0 1 1 6 】

S D R A M バッファ内のホスト C P U でフィルタリングされパケットは、既存のハードウェア D M A 処理によって A / V キュー (A/V Queue) に転送され、P V R の動作を模倣する。

【 0 1 1 7 】

セットトップボックスの第 2 の構成例を図 1 5 に示す。デコーダ I C 9 3 0 内の R I S C プロセッサ A / V デコーダモジュール 9 3 4 は、パーシャルトランスポート P I D を処理し、デコードのための抽出及び結合を行うので、デコーダ I C 9 3 0 内のファームウェアは、各パケットヘッダ内の基準に基づいて、パーシャルトランスポートストリーム内の個々のパケットを除外することができる。これに代えて、デマルチプレクサ 9 1 0 によってパケットを除外するように設計してもよい。旧式の方式によってスクランブルされたパケットは、暗号化されたまま、C A モジュールを通過する。デコーダ I C 9 3 0 を用いて、旧式の方式によってスクランブルされたパケットを取り除くことによって、及び新たな暗号化アルゴリズム (例えば、N D S) によって暗号化されているパケットが旧式の方式で暗号化されたパケットに隣接して存在すると (又は、少なくとも次の第 1 のストリームビデオパケットより先に配置されていると) 仮定すると、旧式のパケットの除外により、事実上、単一のクリアなストリームがヘッダストリップ及びビデオキューにマージされることとなる。

【 0 1 1 8 】

セットトップボックスにおいて、部分暗号化を行うための第 3 の構成例を図 1 6 に示す。この実施例では、チューナ及び復調器 9 0 4 とデコーダ I C 9 0 8 との間に設けられた特定用途向け集積回路 (Application Specific Integrated Circuit : A S I C)、フィールドプログラマブルゲートアレイ (Field Programmable Gate Array : F P G A)、プログラマブルロジックデバイス (programmable logic device : P L D) 9 3 8 又はこの他の専用に設計された回路によって P I D 再マッピングを行う。この実施例の変形例として、デコーダ I C 9 0 8 を変更し、P I D 再マッピングをデマルチプレクサ 9 4 0 内で行うようにしてもよい。いずれの場合も、旧式の方式によって暗号化されたパケットは除外され、非旧式のパケットが回路 9 3 8 又はデマルチプレクサ 9 4 0 で再マッピングされる。

【 0 1 1 9 】

この第3の手法は、一実施例においては図17に示すPLDを用いて実現してもよい。この実施例では、特定のPIDを有する暗号化されたパケットは、連続して最大1個までしか現れないと仮定し、したがって（後述するように）、例えば、上述したM番目N暗号化構成とともに、暗号化されたパケットのバーストに対応するように構成を変更する。入力ストリームは、PIDに基づいて、入力ストリームを逆多重化するPID判別器950を通過する。連続カウンタ確認器958は、第1のPIDパケットの連続性を確認する。連続性にエラーが検出された場合、ブロック960において、このエラーが検出され、カウンタがリセットされる。

【0120】

元の入力パケットストリームは、多数のPIDによってタグが付されたパケットを含む。PID判別器950は、所定の2つのPID（第1及び第2のPID）を有するパケットを他の全てのパケットから分離する。この機能は、複数の対を処理するように拡張してもよい。これらの他のパケットは、変更された（revised）出力ストリームに直接バイパスされる。この処理では、3バイト又は4バイトのクロック遅延が生じる。

【0121】

第2のPIDを有するパケットは、PID判別器950によって、連続カウンタ確認器954にルーティングされ、連続カウンタ確認器594は、このPIDについて、シーケンスの完全性を検証する。ブロック956は、エラーを検出するが、このエラーの処理は、本発明に直接関係しないため詳細には説明しない。パケットの連続性を示す値は、後のパケットのシーケンスの確認に使用するために保存される。連続カウンタ確認器958は、独立した第1のカウンタを用いて、第1のPIDを有するパケットについて、対応する連続性を確認し、ここでも、ブロック960においてエラーが検出される。

【0122】

ブロック962において、第2のパケットに第2のフラグがあるか否かが判定される。このブールインジケータ（Boolean indicator）は、直前のクリアなパケット以来、第2のパケットが処理されていることを記憶するために用いられる。この実施例では、クリアなパケット間に2つ以上の第2のパケットがあるとエラーとなり、ブロック964において、このエラーが検出される。第2のパケットの存在は、ブロック966において、第2のフラグを設定することによって以後の処理に示される。

【0123】

第2のパケットの連続カウンタは、ブロック968において、クリアなパケットのシーケンスに適合するように変更される。ブロック958において、この置換（substitution）のためのデータは、連続カウンタ確認器958において第1のストリームの連続性を検証するために用いた値に由来する。変更されたパケットは、ブロック968から出力され、変更されたストリームにマージされ、これにより出力ストリームが生成される。

【0124】

第1のPIDを有するパケットが連続カウンタ確認器958において、連続性を確認された後、これらのパケットは、ブロック970において、ヘッダ内のスクランブルフラグ（scrambling flag）によって区別される。パケットがスクランブルされている場合、ブロック974において、第1のフラグが要求される。この第1のフラグであるブールインジケータは、直前のクリアなパケット以来、第1のパケットが処理されていることを記憶するために用いられる。この実施例では、クリアなパケット間に2つ以上の第1のパケットがあるとエラーとなり、ブロック976において、このエラーが検出された後、ブロック978においてパケットが削除される。第1のパケットの存在は、ブロック978において、第1のフラグを設定することによって以後の処理に示される。暗号化されたパケットを使用するユーザがダウンストリーム側にいない場合、ブロック978において、このパケットを削除してもよい。幾つかの状況では、このパケットを継続する必要がある場合がある（この場合、その連続カウンタは、除外して第2の継続値を用いることができる）。

【0125】

ブロック 970 における第 1 の P I D のスクランブル検査によって、クリアなパケットが検出された場合、ブロック 984 において、第 2 及び第 1 のフラグの状態が検査される。暗号化されたパケットは、常に対として存在するため、有効となる条件は、この対の両方が存在しない場合か、両方が存在する場合のいずれかである。これらの対のうち的一方のみが存在する状況は、ブロック 988 においてエラーと判定される。但し、この実施例では、出現の順序は問題としない。なお、第 1 のパケットに削除のためのフラグを付す手法としては、例えばトランスポートプライオリティビット (TRANSPORT_PRIORITY) 等のトランスポートヘッダのビットをスクランブルしてもよく、これ以外の手法を用いてもよい。更に、如何なるビットも使用せず、例えば、第 1 (第 2) のパケットが第 2 (第 1) のパケットの前にあるか後にあるかといった第 1 (第 2) のパケットの単純な位置情報をインジケータとして用いてもよい。

【 0 1 2 6 】

第 1 の P I D を有するクリアなパケットの P I D 値は、ブロック 992 において、第 2 の P I D に変更された後、変更された出力ストリームに組み込まれる。これに代えて、第 2 の P I D を有するパケットを第 1 の P I D 値に再マッピングしてもよい。コンテンツをデコードするための正しい P I D (第 1 の又は第 2 の P I D のいずれか) がデコーダに供給されると、コンテンツをデコードすることができる。クリアなパケットの存在は、第 1 又は第 2 のブルフラグによって示される。

【 0 1 2 7 】

上述した全ての実施例において、一連の第 1 のパケットに置換のためのタグが付されていても、第 2 のパケットを置換すべき第 1 のパケットに隣り合うように挿入することができる。なお、幾つかの実施例では、第 2 のパケットを介在させることなく、複数の暗号化パケットをストリームに挿入できる場合、ヘッドエンド部分スクランブルを行ってもよい。(例えば、M 番目 N 部分暗号化方式のように) 複数の連続する暗号化されたパケットをストリームに含ませるために、第 1 及び第 2 のフラグの使用を、カウンター一致検査機能 (counter matching test function) に置き換えてもよい。この場合、ブロック 962、964、966 に代えて、第 2 の暗号化パケットカウンタをインクリメントする。また、ブロック 970、974、976、980 に代えて、第 1 の暗号化パケットカウンタをインクリメントする。ブロック 984 は、第 1 及び第 2 のパスから、同じ数の暗号化されたパケットが受け取られていることを確認するための第 1 及び第 2 の暗号化パケットカウンタの比較に置き換えられる。また、ブロック 992 においてフラグを消去するのに代えて、ここでは、カウンタをリセットするこの変形例により、複数の暗号化パケットを継続的に受け取ることができ、受け取られたパケットの数を比較して、データストリームの完全性を監視することができる。当業者は、この他の変形例を想到することもできる。

【 0 1 2 8 】

図 17 を用いて上述した機能は、市販されているセットトップボックスにおいて使用されており、市場から入手することができるブロードコム (Broadcom) シリーズ 70 x x 又は 71 x x デコーダの機能と同等の機能を有する A / V デコーダチップに統合してもよい。図 18 は、このようなデコーダチップのブロック図であり、ここでは、市販されているチップにおいて既に設けられている機能は、基本的に変更していない。通常、市販されているデコーダチップは、P I D と番組コンポーネント (例えば、オーディオ、ビデオ) との間に対一の対応関係があることを前提に設計されている。

【 0 1 2 9 】

図 18 に示すデコーダは、メインオーディオと、メインビデオと、ピクチャインピクチャ (picture-in-picture: P i P) 機能に用いるセカンダリビデオとについて、第 1 及び第 2 の P I D を処理できるように、S T B の C P U への接続を介して、複数の P I D がデコーダにプログラミングされることを許容するこの実施例では、生のデータストリームが図 17 を用いて上述した、P I D に基づいてパケットのストリームを逆多重化する機能と同様の機能を有するパケットソータ 1002 によって受け取られる。好ましくは、図 18 に示すデコーダは、プログラミングされたソフトウェアではなく、ハードワイヤード論理

回路を用いて、パケットソータ1002におけるPIDソート機能を実現する。番組ガイド及びストリームナビゲーション情報は、例えば、STBのCPUによって使用するために出力される。メインオーディオ番組に関連するパケットは、FIFO1006内にバッファリングされた後、復号器1010によって復号され、バッファ1014にバッファリングされ、MP EGオーディオデコーダ1018によって、必要なときに読み出される。デコードされたMP EGオーディオ信号は、デコーダからの出力信号として出力される。

【0130】

同様に、メインビデオ番組に関連するパケットは、FIFO1024内にバッファリングされた後、復号器1028によって復号され、バッファ1032にバッファリングされ、MP EGビデオデコーダ1036によって、必要なときに読み出される。メインチャンネルのデコードされたMP EGビデオ信号は、後述する混合器 (compositer) 1040に供給され、ここから、デコーダからの出力信号として出力される。同様に、ピクチャインピクチャビデオに関連するパケットは、FIFO1044内にバッファリングされた後、復号器1048によって復号され、バッファ1052にバッファリングされ、MP EGビデオデコーダ1056によって、必要なときに読み出される。ピクチャインピクチャチャンネルのデコードされたMP EGビデオ信号は、混合器1040に供給され、ここで、メインチャンネルビデオ信号と合成され、ここから、デコーダからの出力信号として出力される。メインチャンネル又はピクチャインピクチャチャンネルに関連しない他のパケットは削除される。勿論、本発明の範囲から逸脱することなく、他の機能をデコーダチップに組み込み、又はデコーダチップから既存の機能を削除してもよい。

【0131】

結論

上述のように、ハッカーからの執拗な攻撃に対抗するために、上述した部分暗号化構成の幾つかを組み合わせ、更に安全性を高めてもよい。例えば、クリティカルパケット暗号化は、安全性を高めるために、SI暗号化、M番目N暗号化、ランダム暗号化、タイムスライス暗号化、及び他の手法のいずれと組み合わせてもよい。一実施例においては、帯域幅が許す限り、可能な限り多くのパケットを暗号化する。暗号化の量は、コンテンツがレギュラー番組であるか、プレミア番組 (例えば、ペイパービュー又はVOD) であるか、コンテンツがアダルト番組であるか通常の映画であるか、或いは、様々なケーブルオペレータが適当と認める安全性のレベルに応じて決定してもよい。本発明の範囲から逸脱することなく、暗号化の安全性を更に高めるために他の様々な組合せが可能であることは、当業者にとって明らかである。

【0132】

上述した様々な実施例では、MP EG 2符号化を用いたデジタルA/Vシステムに関連して本発明を説明した。したがって、様々なパケット名及びプロトコルとしては、MP EG 2符号化及び復号に関連するものを用いた。しかしながら、ここに開示し、特許を請求する概念は、このような範囲に限定されるものではないことは当業者にとって明らかである。同様の又は類似する手法は、MP EG 2プロトコルに限定されることなく、如何なるデジタルケーブルシステムにおいても実現できる。更に、本発明の手法は、例えば、以下に限定されるものではないが、地上波放送を用いたコンテンツ配信方式、インターネットを用いたコンテンツ配信方式、例えば、DirectV (商標) 等で用いられているデジタル衛星サービス (Digital Satellite Service: DSS) 等の衛星を用いたコンテンツ配信方式、及びパッケージ媒体 (例えば、CDやDVD) を含む他の適切な如何なるコンテンツ配信シナリオにおいて実現してもよい。これらに基づく様々な変形例は、ここに説明した技術と等価であり、ここに例示的に説明したMP EG 2ケーブルシステムの実施例は、本発明を例示的に説明するための一具体例と解釈するべきである。

【0133】

更に、テレビジョンセットトップボックスを用いて、部分的に暗号化されたテレビジョン番組を復号する具体例によって本発明を説明した。しかしながら、本発明に基づく復号メカニズムは、STBを備えないテレビジョン受信機においても同様に実現でき、更に、

M P 3 プレイヤ等のミュージックプレイヤにおいても実現できる。これらの実施例も、ここに説明した実施例と等価である。

【 0 1 3 4 】

更に、テレビジョン番組のデュアル部分暗号化のためのメカニズムを提供するための暗号化方式に関連して本発明を説明したが、部分暗号化方式は、単一の暗号化方式、又は2つ以上の暗号化方式における複数の暗号化方式としても制限なく用いることができる。暗号化された更なる複製されたパケットに2つ以上の暗号化方式を適用してもよい。また、複製されたパケットの1つのための暗号化鍵を複数の暗号化方式間で共有してもよい。更に、ここでは、特にテレビジョン番組の暗号化を行う特別な目的について説明したが、本発明は、以下に限定されるものではないが、インターネット又は他のネットワークからダウンロードされるコンテンツ、音楽コンテンツ、パッケージ媒体、及びこれらの他の種類の情報コンテンツを含む他のコンテンツを単独で暗号化し又はデュアル部分暗号化するために用いてもよい。更に、本発明の範囲から逸脱することなく、これらのコンテンツは、以下に限定されるものではないが、例えば、携帯情報端末 (personal digital assistant : P D A)、パーソナルコンピュータ、個人用ミュージックプレイヤ、オーディオシステム、オーディオ/ビデオシステム等を含む如何なる再生機器において再生してもよい。

【 0 1 3 5 】

当業者には明らかであるが、ここでは、プログラミングされたプロセッサを用いて実現できる例示的な実施例を用いて本発明を説明した。しかしながら、本発明は、このような実施例に限定されるわけではなく、本発明は、特定用途のハードウェア等のハードウェアコンポーネントの等価物を用いても実現でき、及び/又は専用のプロセッサを用いても実現でき、このような実現例は、ここに開示し、請求の範囲において請求する本発明と等価である。同様に、汎用コンピュータ、マイクロプロセッサを用いたコンピュータ、マイクロコントローラ、光コンピュータ、アナログコンピュータ、専用プロセッサ、及び/又は専用ハードワイヤード論理回路を用いて、本発明の実施例と等価な構成を構築することもできる。

【 0 1 3 6 】

また、上述の実施例を実現するためのプログラミングのステップ及びこれらに関連するデータは、本発明の範囲を逸脱することなく、読出専用メモリ (Read Only Memory : R O M) 素子、ランダムアクセスメモリ (Random Access Memory : R A M) 素子、光ストレージ装置、磁気ストレージ装置、光磁気ストレージ装置、フラッシュメモリ、コアメモリ、及び/又はこの他の同等のストレージ技術を用いても実現できる。これらと同様のストレージ装置は、等価物とみなすことができる。

【 0 1 3 7 】

本発明は、先にフローチャートを用いて広く説明し、適切な電子ストレージ媒体に格納でき、又は適切な電子通信媒体を介して伝送できるプログラミング命令を実行するプログラミングされたプロセッサを用いて実現することができる。なお、上述した処理は、本発明の範囲を逸脱することなく様々に変形でき、様々な適切なプログラミング言語を用いて記述できることは当業者にとって明らかである。例えば、本発明の範囲から逸脱することなく、実行される動作の順序を変更でき、他の動作を加えることも幾つかの動作を省略することもできる。また、本発明の範囲を逸脱することなく、エラー修正処理を追加及び/又は拡張してもよく、ユーザインタフェース及び表示される情報を様々に変更してもよい。これらの変形も等価であるとみなされる。

【 0 1 3 8 】

本発明を特定の具体例を用いて説明してきたが、当業者は、上述の説明から多くの代替例、修正例、変更例、変形例を想到することができる。これらの代替例、修正例、変更例、変形例は、本発明の範囲内にある。

【 手 続 補 正 2 】

【 補 正 対 象 書 類 名 】 特 許 請 求 の 範 囲

【 補 正 対 象 項 目 名 】 全 文

【補正方法】変更**【補正の内容】****【特許請求の範囲】****【請求項 1】**

コンテンツを暗号化する暗号化方法において、

上記コンテンツの100%未満を暗号化する選択アルゴリズムに基づいて暗号化するコンテンツの部分を特定するステップと、

上記特定されたコンテンツの部分を第1の暗号化方式に基づいて暗号化して、第1の暗号化された部分を生成するステップと、

上記特定されたコンテンツの部分を第2の暗号化方式に基づいて暗号化して、第2の暗号化された部分を生成するステップと、

暗号化されていない部分とともに、上記第1の暗号化された部分と、第2の暗号化された部分とを結合して、部分多重暗号化コンテンツを生成するステップとを有する暗号化方法。

【請求項 2】

上記コンテンツは、デジタルビデオ信号を有することを特徴とする請求項1記載の暗号化方法。

【請求項 3】

上記部分多重暗号化テレビジョン信号を、ケーブルシステム、地上波放送システム、衛星システム、パッケージ媒体のいずれかを介して、配信するステップを更に有する請求項1又は2記載の暗号化方法。

【請求項 4】

上記コンテンツは、第1の packets 識別子を用いて packets 化され、暗号化のために選択されるコンテンツを含む packets の packets 識別子は、第2の packets 識別子にマッピングされることを特徴とする請求項1乃至3いずれか1項記載の暗号化方法。

【請求項 5】

packets 化されたデジタルテレビジョン信号を符号化する符号化方法において、

第1の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含む packets の一部を暗号化するステップと、

第2の暗号化アルゴリズムに基づき、デジタルテレビジョン信号を含む packets の一部を暗号化するステップと、

デジタルテレビジョン信号を含む packets の一部を暗号化せずにそのまま残すステップと、

上記暗号化されていない packets に第1の packets 識別子を割り当てるステップと

上記第1の暗号化アルゴリズムに基づいて暗号化された packets に第1の packets 識別子を割り当てるステップと、

上記第2の暗号化アルゴリズムに基づいて暗号化された packets に第2の packets 識別子を割り当てるステップとを有する符号化方法。

【請求項 6】

上記デジタルテレビジョン信号を上記第1及び第2の packets 識別子にリンクする情報を生成するステップを更に有する請求項5記載の符号化方法。

【請求項 7】

上記デジタルテレビジョン信号を上記第1及び第2の packets 識別子にリンクする情報を番組特定情報として送信するステップを更に有する請求項6記載の符号化方法。

【請求項 8】

ケーブルシステム、地上波放送システム、衛星システムのいずれかを介して、上記暗号化されていない packets を、上記第1及び第2の暗号化アルゴリズムに基づいて暗号化された packets とともに送信するステップを更に有する請求項5乃至7いずれか1項記載の符号化方法。

【請求項 9】

衛星信号デスクランブラからクリアなパケットのストリームを受信する入力手段と、
多重暗号化するパケットのグループを選択するとともに、クリアなパケットの組を残す
選択手段と、

上記選択されたパケットを複製し、第1及び第2の複製されたパケットの組を生成する
複製手段と、

第1のパケット識別子を第1の複製されたパケットの組に割り当て、第2のパケット識
別子を第2の複製されたパケットの組に割り当てる割り当て手段と、

上記第1の複製されたパケットの組と、上記第2の複製されたパケットの組と、上記ク
リアなパケットの組とを多重化してパケットの出力ストリームを生成する多重化手段とを
備えるパケット選択及び複製装置。

【請求項10】

第1の暗号化アルゴリズムに基づいて、上記第1のパケット識別子を有するパケットを
暗号化する第1の暗号化器を更に備える請求項9記載のパケット選択及び複製装置。

【請求項11】

第2の暗号化アルゴリズムに基づいて、上記第2のパケット識別子を有するパケットを
暗号化する第2の暗号化器を更に備える請求項9又は10記載のパケット選択及び複製装
置。

【請求項12】

上記第1の複製されたパケットの組と上記クリアなパケットの組とが同じパケット識
別子に割り当てられるようにパケット識別子を再マッピングするパケット再マッピング手
段を更に備える請求項9乃至11いずれか1項記載のパケット選択及び複製装置。

【請求項13】

第1のパケット識別子を有するクリアなパケットと、第2のパケット識別子を有する暗
号化されたパケットと、第3のパケット識別子を有する暗号化されたパケットとからなる
変調パケットのストリームを復調する復調器と、

上記第1のパケット識別子を有するクリアなパケットと、上記第2のパケット識別子を
有する暗号化されたパケットとが同じパケット識別子を有するように上記パケット識別
子を変更する再マッピング器とを備えるパケット識別子再マッピング装置。

【請求項14】

上記第3のパケット識別子を有するパケットは、クリアなパケットを含み、上記第2の
パケット識別子を有するパケットを暗号化するアルゴリズムとは異なるアルゴリズムで、
該第3のパケット識別子を有するパケットを暗号化する暗号化器を更に備える請求項13
記載のパケット識別子再マッピング装置。

【請求項15】

上記再マッピングされたパケットを上記第3のパケット識別子を有するパケットに結合
して、出力データストリームを生成するマルチプレクサを更に備える請求項13又は14
記載のパケット識別子再マッピング装置。

【請求項16】

上記変調パケットのストリームは、システム情報を有するパケットを含み、

上記第3のパケット識別子を有するパケットを暗号化した暗号化法を特定するように上
記システム情報を変更する変更手段を更に備える請求項13乃至15いずれか1項記載の
パケット識別子再マッピング装置。

【手続補正3】

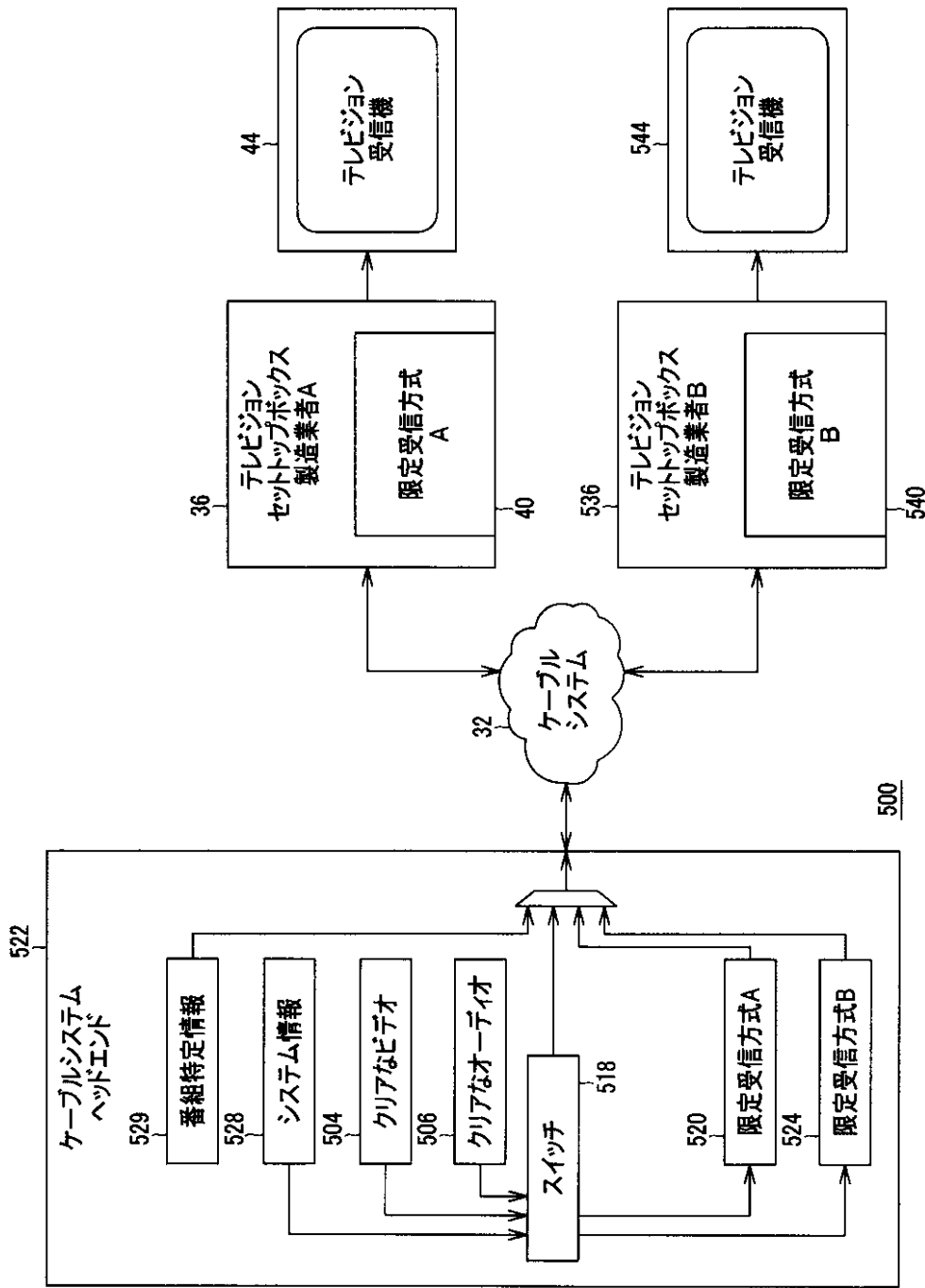
【補正対象書類名】図面

【補正対象項目名】図10

【補正方法】変更

【補正の内容】

【図 10】



【手続補正書】

【提出日】平成21年12月11日(2009.12.11)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

衛星信号デスクランブラからクリアなパケットのストリームを受信する入力手段と、多重暗号化するパケットのグループを選択するとともに、クリアなパケットの組を残す

選択手段と、

上記選択されたパケットを複製し、第1及び第2の複製されたパケットの組を生成する複製手段と、

第1のパケット識別子を第1の複製されたパケットの組に割り当て、第2のパケット識別子を第2の複製されたパケットの組に割り当てる割り当て手段と、

上記第1の複製されたパケットの組と、上記第2の複製されたパケットの組と、上記クリアなパケットの組とを多重化してパケットの出力ストリームを生成する多重化手段とを備えるパケット選択及び複製装置。

【請求項2】

第1の暗号化アルゴリズムに基づいて、上記第1のパケット識別子を有するパケットを暗号化する第1の暗号化器を更に備える請求項1記載のパケット選択及び複製装置。

【請求項3】

第2の暗号化アルゴリズムに基づいて、上記第2のパケット識別子を有するパケットを暗号化する第2の暗号化器を更に備える請求項1又は2記載のパケット選択及び複製装置

。

【請求項4】

上記第1の複製されたパケットの組と上記クリアなパケットの組とが同じパケット識別子に割り当てられるようにパケット識別子を再マッピングするパケット再マッピング手段を更に備える請求項1乃至3いずれか1項記載のパケット選択及び複製装置。

【請求項5】

第1のパケット識別子又は第2のパケット識別子に関連付けられたパケットによって識別される、部分的に暗号化されたテレビジョン信号を受信する受信手段と、

上記第2のパケット識別子を有するパケットを復号する復号器と、

上記第1のパケット識別子を有するパケットとともに上記第2のパケット識別子を有するパケットをデコードすることにより、上記部分的に暗号化されたテレビジョン信号をデコードするデコーダとを備えるテレビジョン受信機。

【請求項6】

上記第1のパケット識別子を有する暗号化されたパケットを除外する除外手段を備える請求項5記載のテレビジョン受信機。

【請求項7】

上記第1のパケット識別子に関連付けられたパケットは、第1の暗号化方式に基づいて暗号化されており、上記第2のパケット識別子に関連付けられたパケットは、第2の暗号化方式に基づいて暗号化されていることを特徴とする請求項5記載のテレビジョン受信機

。

【請求項8】

テレビジョン装置、テレビジョン受信装置及び集積回路の1つ以上に内蔵されることを特徴とする請求項5乃至7記載のテレビジョン受信機。

フロントページの続き

(74)代理人 100109335

弁理士 上杉 浩

(74)代理人 100158551

弁理士 山崎 貴明

(72)発明者 カンデロア、ブランド、エル .

アメリカ合衆国 カリフォルニア州 92029-6502 エスコンディード クウェイル グ
レン ウェイ 10124

(72)発明者 アンガー、ロバート、アラン

アメリカ合衆国 カリフォルニア州 92019 エルカホン ヴィスタ ハーモース ウェイ
2072

(72)発明者 ペドロウ、レオ、エム .、ジュニア

アメリカ合衆国 カリフォルニア州 92065 ラモナ ガージャン レーン 17193

Fターム(参考) 5C164 FA03 PA13 SA31S SB03P SB15S SC02P TB23S TB24S UA03S UB03P

UB21S UB24S UC22P

5J104 AA32 AA33 AA34 BA03 JA03 NA02 NA37 PA05