【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年2月9日(2006.2.9)

【公表番号】特表2005-514886(P2005-514886A)
【公表日】平成17年5月19日(2005.5.19)
【年通号数】公開・登録公報2005-019
【出願番号】特願2003-559216(P2003-559216)
【国際特許分類】
Ｈ０４Ｎ　7/167　(2006.01)
Ｈ０４Ｎ　7/16　(2006.01)
Ｈ０４Ｌ　9/18　(2006.01)
【ＦＩ】
Ｈ０４Ｎ　7/167　Ｚ
Ｈ０４Ｎ　7/16　Ａ
Ｈ０４Ｌ　9/00　６５１

【手続補正書】
【提出日】平成17年12月13日(2005.12.13)
【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】
暗号化されていないテレビジョン信号を暗号化する暗号化方法において、
上記暗号化されていないテレビジョン信号を特定された時間的間隔でサンプリングするステップと、
各サンプルに対して、
第１の暗号化方式に基づいて該サンプルを暗号化して、第１の暗号化サンプルを生成するステップと、
第２の暗号化方式に基づいて該サンプルを暗号化して、第２の暗号化サンプルを生成するステップとを有する暗号化方法。
【請求項２】
上記第１及び第２の暗号化サンプルを上記暗号化されていないテレビジョン信号のサンプリングされていない部分に結合して、部分多重暗号化テレビジョン信号を生成するステップを更に有する請求項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、通信媒体を介して配信するステップを更に有する請求項２記載の暗号化方法。
【請求項４】
上記第１の暗号化サンプル、第２の暗号化サンプル及び部分多重暗号化テレビジョン信号のサンプリングされていない部分を、複数のパケット識別子を割り当てることによって識別するステップを更に有する請求項２記載の暗号化方法。
【請求項５】
上記テレビジョン信号の暗号化されていない部分に、第１のパケット識別子を割り当てるステップと、
上記第１の暗号化方式に基づいて暗号化されたサンプルに、上記第１のパケット識別子を割り当てるステップと、

上記第２の暗号化方式に基づいて暗号化されたサンプルに、第２のパケット識別子を割り当てるステップとを更に有する請求項１記載の暗号化方法。
【請求項６】
上記特定された時間的間隔は、ランダムな時間的間隔であることを特徴とする請求項１記載の暗号化方法。
【請求項７】
上記特定された時間的間隔は、上記テレビジョン信号の各Ｍ個の期間におけるＮ個の期間であることを特徴とする請求項１記載の暗号化方法。
【請求項８】
上記Ｎ個の期間及びＭ個の期間は、ランダムに選択されることを特徴とする請求項７記載の暗号化方法。
【請求項９】
デジタルテレビジョン信号を処理するテレビジョン信号処理方法において、
上記デジタルテレビジョン信号の第１の暗号化サンプルであって、任意の時間的間隔に基づいて選択され、第１の暗号化方式に基づいて暗号化された第１の暗号化サンプルと、上記デジタルテレビジョン信号の第２の暗号化サンプルであって、任意の時間的間隔に基づいて選択され、第２の暗号化方式に基づいて暗号化された第２の暗号化サンプルと、暗号化されていない部分とを有するデジタルテレビジョン信号を受信するステップと、
上記第１の暗号化サンプルを復号して、復号サンプルを生成するステップと、
上記暗号化されていない部分と上記復号サンプルとをデコードするステップとを有するテレビジョン信号処理方法。
【請求項１０】
上記第１の暗号化サンプルは、第１のパケット識別子によって識別され、上記第２の暗号化サンプルは、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９記載のテレビジョン信号処理方法。
【請求項１１】
上記時間的間隔は、ランダムな時間的間隔であることを特徴とする請求項９又は１０記載のテレビジョン信号処理方法。
【請求項１２】
上記時間的間隔は、上記テレビジョン信号の各Ｍ個の期間におけるＮ個の期間であることを特徴とする請求項１１記載のテレビジョン信号処理方法。
【請求項１３】
上記Ｎ個の期間及びＭ個の期間は、ランダムに選択されることを特徴とする請求項１２記載のテレビジョン信号処理方法。
【請求項１４】
テレビジョン装置、テレビジョン受信機、テレビジョンセットトップボックス及び集積回路の１つにおいて実行されることを特徴とする請求項９乃至１３記載のテレビジョン信号処理方法。
【請求項１５】
デジタルテレビジョン信号をデコードするテレビジョン受信機において、
任意の時間的間隔に基づいて選択され、第１の暗号化方式に基づいて暗号化された第１の暗号化サンプルと、任意の時間的間隔に基づいて選択され、第２の暗号化方式に基づいて暗号化された第２の暗号化サンプルと、暗号化されていない部分とを有するテレビジョン信号を受信する受信機と、
上記第１の暗号化サンプルを復号して、復号サンプルを生成する復号器と、
上記暗号化されていない部分と上記復号サンプルと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１６】
上記第１の暗号化サンプルは、第１のパケット識別子によって識別され、上記第２の暗号化サンプルは、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１５

記載のテレビジョン受信機。
【請求項１７】
上記時間的間隔は、ランダムな時間的間隔であることを特徴とする請求項１５又は１６記載のテレビジョン受信機。
【請求項１８】
上記時間的間隔は、上記テレビジョン信号の各Ｍ個の期間におけるＮ個の期間であることを特徴とする請求項１７記載のテレビジョン受信機。
【請求項１９】
上記Ｎ個の期間及びＭ個の期間は、ランダムに選択されることを特徴とする請求項１８記載のテレビジョン受信機。
【請求項２０】
テレビジョン装置、テレビジョン受信機、テレビジョンセットトップボックス及び集積回路の１つに内蔵されていることを特徴とする請求項１５乃至１９記載のテレビジョン受信機。
【手続補正２】
【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】
【発明の名称】時間分割部分暗号化
【関連出願】
【０００１】
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。
【０００２】
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第１０／０３７，９１４号、代理人整理番号ＳＮＹ-Ｒ４６４６．０３「エレメンタリストリーム部分暗号化（Elementary Stream Partial Encryption）」、アンガー他の米国特許出願第１０／０３７，４９９号、代理人整理番号ＳＮＹ-Ｒ４６４６．０４「部分的な暗号化及びＰＩＤマッピング（Partial Encryption and PID Mapping）」、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）」と同時に出願されて

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。
【著作権表示】
【０００３】
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。
【技術分野】
【０００４】
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。
【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、ＮＤＳ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（米国イリノイ州ショウンバーグ）、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ＣＡ方式を含む幾つかのＣＡ方式が使用されている。ＣＡ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ＳＴＢの製造業者は、このＳＴＢ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ＣＡ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、ＣＡ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ＣＡ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、ＳＴＢ供給元が複数あることを希望する

。
【０００７】
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。ＳＴＢ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。
【０００８】
旧型のＳＴＢ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ＣＡ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ＣＡ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ＳＴＢ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。
【０００９】
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２２において方式Ａに準拠したＣＡ暗号化装置１８を用い、製造業者Ａ（方式Ａ）のＣＡ技術によってオーディオ／ビデオ（Ａ／Ｖ）コンテンツ１４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ＳＩという。）２６及び番組特定情報（program specific information：以下ＰＳＩという。）２７が多重化され、ケーブルシステム３２を介してユーザのＳＴＢ３６に伝送される。ＳＴＢ３６には、暗号化されたＡ／Ｖコンテンツを復号するＣＡ方式Ａ（製造業者Ａ）のＣＡ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４４に供給され、ユーザによって視聴される。
【００１０】
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ＰＩＤ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もよい。
【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。

【発明の開示】

【課題を解決するための手段】

【００１３】

本発明に係る暗号化されていないテレビジョン信号を暗号化する暗号化方法において、暗号化されていないテレビジョン信号を特定された時間的間隔でサンプリングし、各サンプルに対して、第１の暗号化方式に基づいてサンプルを暗号化して、第１の暗号化サンプルを生成し、第２の暗号化方式に基づいてサンプルを暗号化して、第２の暗号化サンプルを生成する。

【００１４】

本発明に係るデジタルテレビジョン信号を処理するテレビジョン信号処理方法において、デジタルテレビジョン信号の第１の暗号化サンプルであって、任意の時間的間隔に基づいて選択され、第１の暗号化方式に基づいて暗号化された第１の暗号化サンプルと、デジタルテレビジョン信号の第２の暗号化サンプルであって、任意の時間的間隔に基づいて選択され、第２の暗号化方式に基づいて暗号化された第２の暗号化サンプルと、暗号化されていない部分とを有するデジタルテレビジョン信号を受信し、第１の暗号化サンプルを復号して、復号サンプルを生成し、暗号化されていない部分と復号サンプルとをデコードする。

【００１５】

本発明に係るデジタルテレビジョン信号をデコードするテレビジョン受信機は、任意の時間的間隔に基づいて選択され、第１の暗号化方式に基づいて暗号化された第１の暗号化サンプルと、任意の時間的間隔に基づいて選択され、第２の暗号化方式に基づいて暗号化された第２の暗号化サンプルと、暗号化されていない部分とを有するテレビジョン信号を受信する受信機と、第１の暗号化サンプルを復号して、復号サンプルを生成する復号器と、暗号化されていない部分と復号サンプルとをデコードするデコーダとを備える。

【発明を実施するための最良の形態】

【００１６】

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。

【００１７】

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ＣＡ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ＳＴＢ製造業

者のＣＡ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。

【００１８】

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。

【００１９】

ここに開示する部分デュアル暗号化（partial dual encrytpion）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。

【００２０】

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なように、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。

【００２１】

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。

【００２２】

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。

【００２３】

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。

【００２４】

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。

【００２５】

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。

【００２６】

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の部分と比べても）、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の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。

【００２７】

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、良くても、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。

【００２８】

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。

【００２９】

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。

【００３０】

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。

【００３１】

【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１００１
  - PMT 0x1010
- 番組番号１００２
  - PMT 0x1020
- 番組番号１００３
  - PMT 0x1030
- 番組番号１００４
  - PMT 0x1040
- 番組番号１００５
  - PMT 0x1050
- 番組番号１００６
  - PMT 0x1060
- 番組番号１００７
  - PMT 0x1070
- 番組番号１００８
  - PMT 0x1080
- 番組番号１００９
  - PMT 0x1090

【００３２】
以下の具体的な放送番組マップテーブル（program map table：ＰＭＴ）のＰＳＩ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。
【００３３】
【表２】

PID=0x0010 で伝送される PMT PMT 0x0010 - PMT 番組番号１ - PMT セクションバージョン１０ - PCR PID 0x0011 - エレメンタリストリーム 　- 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 　- 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 　- 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 　- CA プロバイダ＃１用の CA 記述子(ECM)
PID=0x1010 で伝送される PMT PMT 0x1010 - PMT 番組番号１０１０ - PMT セクションバージョン１０ - PCR PID 0x0011 - エレメンタリストリーム 　- 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＃２用の CA 記述子(ECM) - 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 (0x0013) 　- 記述子 　- CA プロバイダ＃２用の CA 記述子(ECM)

【００３４】
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。

【００３５】

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るとは言えない。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。

【００３６】

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。

【００３７】

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。

【００３８】

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する（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つの番組のうちの特定の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。

【００３９】

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ＰＩＤ１１１であり、オーディオパケットに対してはＰＩＤ２１１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ＰＩＤ１０２及び第１のオーディオＰＩＤ２０２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。

【００４０】

【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				…

【００４１】

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ＳＴＢ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。

【００４２】

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。

【００４３】

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となってしまう。

【００４４】

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。

【００４５】

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。

【００４６】

【表４】

PID=0x0010で伝送されるPMT
PMT 0x0010
- PMT 番組番号１
- PMT セクションバージョン１０
- PCR PID 0x0011
- エレメンタリストリーム
  - 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ＰＩＤ)
- 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
  - 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ＰＩＤ)

【００４７】

【表５】

CA プロバイダ＃２用の CA 記述子(ECM)

記述子
- 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)

【００４８】

【表６】

CA プロバイダ＃２用の CA 記述子(第２のＰＩＤ)

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

【００４９】

ＣＡ方式Ａに基づいて動作する旧型のＳＴＢ３６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ＳＴＢ２３６は、ＳＩ２２８を受信する。新型のＳＴＢ２３６は、ＰＳＩ２２９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。

【００５０】

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。

【００５１】

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。

【００５２】

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。

【００５３】
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。
【００５４】
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、いずれの復号方式を有するＳＴＢにおいても、画像は基本的に見ることができない。
【００５５】
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。
【００５６】
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ッジに対して、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のシャドーＰＩＤ（shadow PID）があるが、特定のＳＴＢ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）を無視することは、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。
【００５７】
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。

【００５８】

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、コンテンツア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。

【００５９】

【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			…
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	…

【００６０】

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。

【００６１】

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（ＣＣＣＣＣＥＥＣＣＥＣＣＣＣＣＥＥＣＣＥ・・・）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。

【００６２】

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。

【００６３】

【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				EB									…
6	PID 116	EB										EB		…
7	PID 117		EB										EB	…
8	PID 118		EB										EB	…
9	PID 119	EB										EB		…

【００６４】

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テ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。

【００６５】

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。

【００６６】

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。

【００６７】

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。

【００６８】

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。

【００６９】

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。

【００７０】

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。

【００７１】

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。

【００７２】

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。

【００７３】

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試みても、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。

【００７４】

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。

【００７５】

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。

【００７６】
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。ＰＥＳ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ＣＡ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ＰＩＤ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ＳＴＢは、それぞれの基本的なＣＡ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。
【００７７】
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ＰＥＳ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、ＰＥＳ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。
【００７８】
ＳＩ暗号化（SI 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（ＳＩ）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、ＳＩ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、ＳＩは、帯域内（in-band）で送信してもよい。帯域内で送信する場合、ＳＩ４２８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ＳＩが、例えばＳＴＢ４３６等の新しいセットトップボックスに供給されるＳＩとが分離されているとする。これにより、ＳＩ４２８の各バージョンは、ＣＡ方式Ａ４１８とＣＡ方式Ｂ４２４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、ＳＩ４２８が必要である。
【００７９】
ＳＩ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、ＳＩ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ＳＩ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。
【００８０】
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、ＰＳＩ４２９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、その番組が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。

【００８１】

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、ＳＩ４２８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ＳＩ４２８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ＳＩ４２８を暗号化する。同時に、クリアなＳＩ４２８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、ＳＩ４２８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ＰＳＩ４２９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ＳＩ（ＳＩ　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。

【００８２】

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。

【００８３】

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、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ＳＩを復号する能力を有する。

【００８４】

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ニングし、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ニング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。

【００８５】

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。

【００８６】

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。

【００８７】

【表９】

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

【００８８】

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。

【００８９】

【表１０】

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

【００９０】

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。

【００９１】

【表１１】

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

【００９２】

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、スクラブリングされた旧型のパケットのＰＩＤ（１２５）をＮＯＰＰＩＤ（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。

【００９３】

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「フォールーブ（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「フォールーブ」のためのＣＡ記述子と、オーディオ基本ＰＩＤ「フォールーブ」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。

【００９４】

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。ＭＰＥＧ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。

【００９５】

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。

【００９６】

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。

【００９７】

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。

【００９８】

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。

【００９９】

ＰＩＤ「Ｂ」及びＰＩＤ「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、ＰＩＤ「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ＰＩＤ再マッピング及びスクランブラ６２０に供給され、ＰＩＤ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ＰＩＤ「Ａ」乃至ＰＩＤ「Ｃ」を再マッピングし、制御方式６２４による制御に基づき、ＮＤＳ暗号化アルゴリズムを用いて、ＰＩＤ「Ｂ」を有するパケットを暗号化する。出力ストリーム６２６は、ＰＩＤ「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ＰＩＤ「Ｃ」を有するパケットと、複製され、選択され、ＮＤＳ暗号化方式によって暗号化されたＰＩＤ「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６２８（例えば、直交振幅変調（quadrature amplitude modulation：以下、ＱＡＭという。）又はＲＦ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（ＰＳＩ）において用いられているオーディオ及びビデオＰＩＤとの互換性を保つために、ＰＩＤ「Ａ」が付された暗号化されていないパケットをＰＩＤ「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、ＰＩＤ「Ｃ」に関する知識のみを有している。これに代えて、ＰＩＤ「Ｃ」が付されたスクランブルされたパケットを逆にＰＩＤ「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ＰＳＩを編集して、ＰＩＤ再マッピング及びスクランブラ６２０においてＰＩＤ「Ｃ」からのＰＩＤ番号をＰＩＤ「Ａ」に振り直す必要がある。

【０１００】

上述の実施例において、ＰＩＤ再マッピング及びスクランブラ６２０は、ＰＳＩ情報の複製に用いることもでき、この場合、ＰＩＤ再マッピング及びスクランブラ６２０は、ＰＳＩ情報を変更して、（ＰＭＴにおけるＣＡ記述を用いて）ＮＤＳ暗号化の追加を反映させ、変更したＰＳＩ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、ＰＩＤ再マッピング及びスクランブラ６２０において、ＮＤＳ暗号化をサポートするＥＣＭ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）。

【０１０１】

このように、ＮＤＳ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ＰＩＤが再マッピングされる。再マッピングされたＰＩＤは、各ＣＡ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ＰＩＤ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ＰＩＤ（又は複数のＰＩＤ）を共有するように再マッピングされる。ＰＩＤ再マッピング及びスクランブラ６２０におけるＰＩＤ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。

【０１０２】

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／デュプリケータ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／デュプリケータ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るべきパケットには、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。

【０１０３】

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／デュプリケータ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。

【０１０４】

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／デュプリケータ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／デュプリケータ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。

【０１０５】

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。

【０１０６】

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ＰＩＤ「Ａ」からＰＩＤ「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ＰＳＩによって処理されるＰＩＤ「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、ＰＩＤ「Ｃ」に関する知識を有するが、ＰＩＤ「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ＰＩＤによって示される。

【０１０７】

上述の実施例において、第２の暗号化方式として用いるＮＤＳ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ＰＩＤ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、ＰＥＳ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ＰＩＤ（例えば、ＰＩＤ「Ｂ」及びＰＩＤ「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ＰＩＤに基づいて暗号化する（すなわち、ＰＩＤ「Ｃ」のパケットは、旧式の暗号化方式に基づいて暗号化し、ＰＩＤ「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ＰＩＤ（例えば、ＰＩＤ「Ａ」）を旧式の方式で暗号化されたパケットのＰＩＤ（ＰＩＤ「Ｃ」）と同じＰＩＤに再マッピングする。

【０１０８】

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。

【０１０９】

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、ＳＴＢには無関係である。

【０１１０】

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、ＲＯＭメモリ９２０に格納されているソフトウェアに基づいて動作するＳＴＢのメインＣＰＵ９１６によって処理される。

【０１１１】

選択されたＰＩＤは、ＳＴＢのＰＩＤ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：ＰＶＲ）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：ＨＤＤ）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、ＳＤＲＡＭという。）にバッファリングされる。ホストＣＰＵ９１６は、「非自動で（manually）」ＳＤＲＡＭ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ＰＩＤ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。

【０１１２】

ホストＣＰＵのオーバヘッドは、ＣＰＵ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、１５Ｍビット／秒のビデオストリームにおける４０ｋ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、１８８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、ＳＤＲＡＭ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ＣＰＵの切換タスクを軽減することができる。

【０１１３】

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ＳＤＲＡＭ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。

【０１１４】

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

【０１１５】

セットトップボックスの第２の構成例を図１５に示す。デコーダＩＣ９３０内のＲＩＳＣプロセッサＡ／Ｖデコーダモジュール９３４は、パーシャルトランスポートＰＩＤ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ＩＣ９３０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９１０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、ＣＡモジュールを通過する。デコーダＩＣ９３０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、ＮＤＳ）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。

【０１１６】

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１６に示す。この実施例では、チューナ及び復調器９０４とデコーダＩＣ９０８との間に設けられた特定用途向け集積回路（Application Specific Integrated Circuit：ＡＳＩＣ）、フィールドプログラマブルゲートアレー（Field Programmable Gate Array：ＦＰＧＡ）、プログラマブルロジックデバイス（programmable logic device ：ＰＬＤ）９３８又はこの他の専用に設計された回路によってＰＩＤ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ＩＣ９０８を変更し、ＰＩＤ再マッピングをデマルチプレクサ９４０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９３８又はデマルチプレクサ９４０で再マッピングされる。

【０１１７】

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。

【０１１８】

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。

【０１１９】

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。

【０１２０】

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。

【０１２１】

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。

【０１２２】

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）。

【０１２３】

ブロック９７０における第１のＰＩＤ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。これらの対のうちの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。

【０１２４】

第１のＰＩＤを有するクリアなパケットのＰＩＤ値は、ブロック９９２において、第２のＰＩＤ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ＰＩＤを有するパケットを第１のＰＩＤ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ＰＩＤ（第１の又は第２のＰＩＤ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。

【０１２５】

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。

【０１２６】

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７０ｘｘ又は７１ｘｘ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、ＰＩＤと番組コンポーネント（例えば、オーディオ、ビデオ）との間に一対一の対応関係があることを前提に設計されている。

【０１２７】

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：ＰｉＰ）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ＰＩＤを処理できるように、ＳＴＢのＣＰＵへの接続を介して、複数のＰＩＤ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、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。

【０１２８】

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（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、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。

【０１２９】

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て、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。

【０１３０】

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。

【０１３１】

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。

【０１３２】

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、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。

【０１３３】

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。

【０１３４】

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。

【０１３５】

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。

【０１３６】

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。

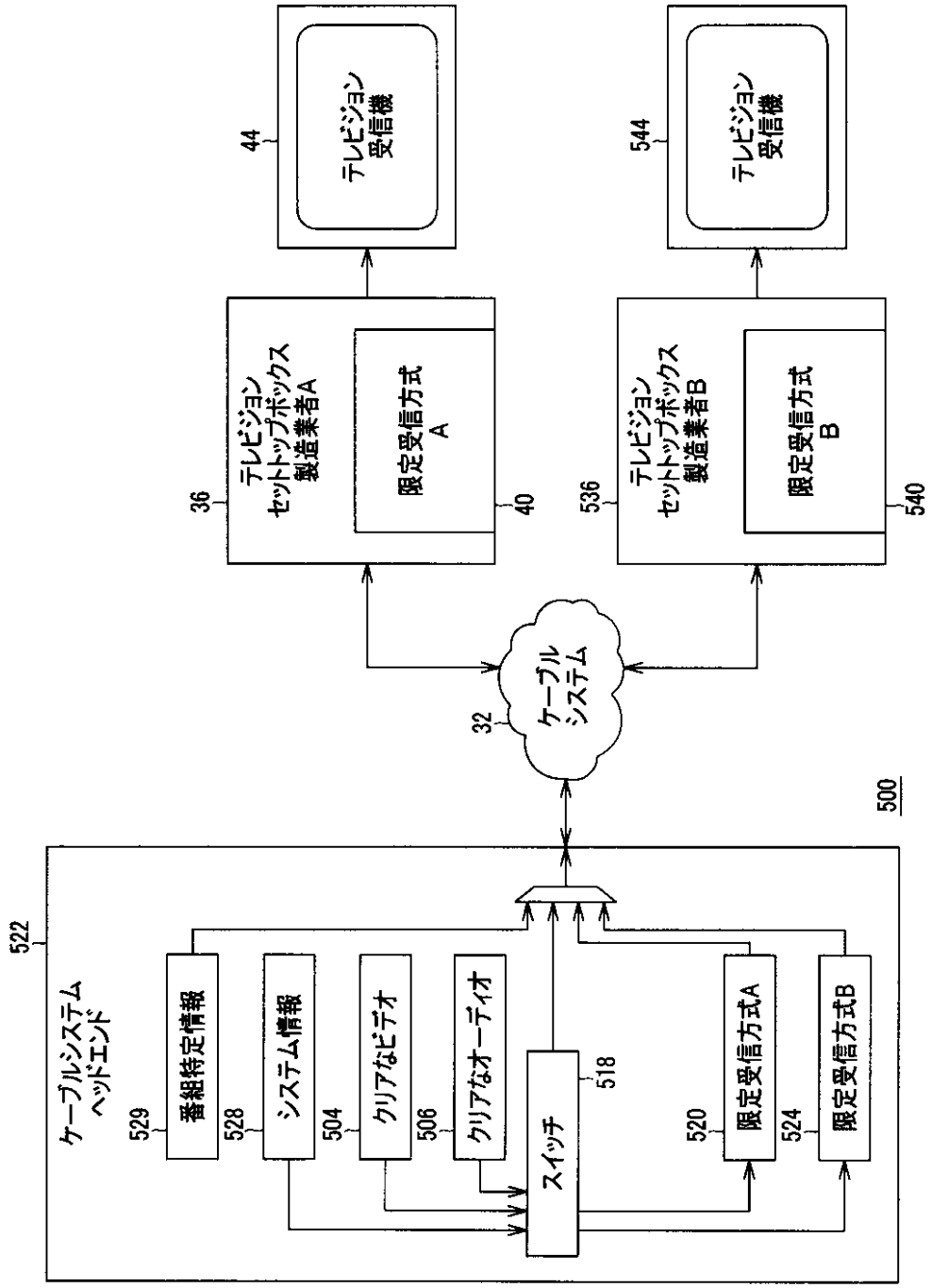
【図面の簡単な説明】

【０１３７】

【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。
【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】


500
ケーブルシステム
ヘッドエンド
522
番組特定情報
529
システム情報
528
クリアなビデオ
504
クリアなオーディオ
506
スイッチ
518
限定受信方式A
520
限定受信方式B
524
ケーブル
システム
32
テレビジョン
セットトップボックス
製造業者A
36
限定受信方式
A
40
テレビジョン
セットトップボックス
製造業者B
536
限定受信方式
B
540
テレビジョン
受信機
44
テレビジョン
受信機
544