(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5551023号
(P5551023)

(45)発行日　平成26年7月16日(2014.7.16)　(24)登録日　平成26年5月30日(2014.5.30)

(51)Int.Cl.　F I
H04N 21/4623 (2011.01)　H04N 21/4623
H04N 21/4385 (2011.01)　H04N 21/4385
H04L 9/36 (2006.01)　H04L 9/00 685

請求項の数 15　外国語出願　(全 16 頁)

(21)出願番号　特願2010-192178(P2010-192178)
(22)出願日　平成22年8月30日(2010.8.30)
(65)公開番号　特開2011-50056(P2011-50056A)
(43)公開日　平成23年3月10日(2011.3.10)
審査請求日　平成25年8月21日(2013.8.21)
(31)優先権主張番号　09168907.5
(32)優先日　平成21年8月28日(2009.8.28)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　500232617
イルデト・ベー・フェー
オランダ・ＮＬ－２１３２・ＬＳ・フーフドドープ・タウルサヴェンウー・１０５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　アンドリュー・アウグスティン・ワイス
オランダ・２０２３・アーアー・ハーレム・ショテルシンゲル・９３

最終頁に続く

(54)【発明の名称】受信器における信頼性があり改竄不可能なデータストリームの処理

(57)【特許請求の範囲】
【請求項１】
受信器(1a)においてヘッダと暗号化されたペイロードとを含むデータストリームを処理する方法であって、前記ヘッダは第１のパケット識別子を含み、
前記方法は、
前記暗号化されたペイロードを解読して解読されたペイロードを取得するステップ(1001)と、
暗号化された第２のパケット識別子と暗号化された第１のコンテンツタイプ識別子とを受け取るステップ(1002)と、
保護された環境内で、前記暗号化された第２のパケット識別子から第２のパケット識別子を取得するステップ(1003)と、
前記保護された環境内で、前記第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を、前記暗号化された第１のコンテンツタイプ識別子から取得するステップ(1004)と、
前記第１のパケット識別子を前記第２のパケット識別子と比較して第１の比較結果を取得するステップ(1005)と、
前記第１の比較結果が第１の所定の条件に合致する場合に、前記第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択し(1007)、かつ、前記解読されたペイロードを復号するために、前記解読されたペイロードを前記第１の復号モジュールに経路指定する(1008)ステップと、

を含む方法。
【請求項２】
前記暗号化された第２のパケット識別子および前記暗号化された第１のコンテンツタイプ識別子は、１つまたは複数の暗号化されたエンタイトルメントメッセージ内で受け取られ、前記第２のパケット識別子および前記第１のコンテンツタイプ識別子は、前記１つまたは複数の暗号化されたエンタイトルメントメッセージをスマートカードに送信(1009)し、かつ、安全な接続を通じて前記スマートカードから前記第２のパケット識別子および前記第１のコンテンツタイプ識別子を受け取る(1010)ことによって取得される請求項１に記載の方法。
【請求項３】
受信器においてヘッダと暗号化されたペイロードとを含むデータストリームを処理する方法であって、前記ヘッダは前記暗号化されたペイロードを識別するための第１のパケット識別子を含み、
前記方法は、
前記暗号化されたペイロードを解読して解読されたペイロードを取得するステップ(1001)と、
保護された環境内で、ハードコードされたメモリから第２のパケット識別子を取得するステップ(1011)と、
前記保護された環境内で、前記第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を、前記ハードコードされたメモリから取得するステップ(1012)と、
前記第１のパケット識別子を前記第２のパケット識別子と比較して第１の比較結果を取得するステップ(1005)と、
前記第１の比較結果が第１の所定の条件に合致する場合に、前記第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択し(1007)、かつ、前記解読されたペイロードを復号するために、前記解読されたペイロードを前記第１の復号モジュールに経路指定する(1008)ステップと、
を含む方法。
【請求項４】
前記ハードコードされたメモリは前記受信器の一部である請求項３に記載の方法。
【請求項５】
前記ハードコードされたメモリはスマートカードの一部である請求項３に記載の方法。
【請求項６】
前記第１のコンテンツタイプ識別子に基づいて予め定義された１組のインターフェースからインターフェースを選択するステップ(1013)と、
前記第１の復号モジュールの出力を前記選択されたインターフェースに制限するステップ(1014)と、
をさらに含む請求項１から５のいずれか一項に記載の方法。
【請求項７】
平文の第３のパケット識別子と、前記第３のパケット識別子に関連付けられた平文の第２のコンテンツタイプ識別子とを受け取るステップ(1015)と、
前記第１の比較結果が第２の所定の条件に合致する場合に、前記第１のパケット識別子を前記第３のパケット識別子と比較して第２の比較結果を取得するステップ(1016)と、
前記第２の比較結果が第３の所定の条件に合致する場合に、前記第２のコンテンツタイプ識別子に基づいて第２の復号モジュールを選択し(1018)、かつ、前記解読されたペイロードを復号するために、前記解読されたペイロードを前記第２の復号モジュールに経路指定する(1019)ステップと、
をさらに含む請求項１から６のいずれか一項に記載の方法。
【請求項８】
前記データストリームはMPEG2トランスポートストリームであり、
前記ヘッダおよび前記暗号化されたペイロードは、前記MPEG2トランスポートストリー

ム内のエレメンタリストリームの一部であり、
前記第３のパケット識別子および前記第２のコンテンツタイプ識別子は、前記MPEG2トランスポートストリーム内のプログラムマップテーブル内で受け取られ、
前記第１の復号モジュールは、前記受信器の保護されたチップセット内の映像デコーダまたは音声デコーダであり、
前記第２の復号モジュールは、前記保護されたチップセットの外部にあるテレテキストデコーダ、サブタイトルデコーダ、またはソフトウェアアプレットである請求項７に記載の方法。
【請求項９】
ヘッダ(101)と暗号化されたペイロード(102)とを含むデータストリームを処理する受信器(1a)であって、前記ヘッダ(101)は第１のパケット識別子(103)を含み、
前記受信器(1a)は、
前記暗号化されたペイロード(102)を解読して解読されたペイロード(104)を取得するように構成されたデスクランブラ(11)と、
暗号化された第２のパケット識別子(105)と暗号化された第１のコンテンツタイプ識別子(106)とを受け取るように構成された第１の入力モジュール(12)と、
プロセッサ(13a)と、
メモリ(14a)と、
ルータ(15)と、
を備え、
前記プロセッサ(13a)は、
前記暗号化された第２のパケット識別子(105)から第２のパケット識別子(107)を取得し、前記暗号化された第１のコンテンツタイプ識別子(106)から前記第２のパケット識別子(105)に関連付けられた第１のコンテンツタイプ識別子(108)を取得し、
前記第２のパケット識別子(107)および前記第１のコンテンツタイプ識別子(108)をメモリ(14a)に記憶し、
前記第１のパケット識別子(103)を前記メモリ(14a)に記憶された前記第２のパケット識別子(107)と比較して第１の比較結果を取得し、
前記第１の比較結果が第１の所定の条件に合致する場合に、前記第１のコンテンツタイプ識別子(108)を前記ルータ(15)に供給するように構成され、
前記ルータ(15)は、
前記第１のコンテンツタイプ識別子(108)に基づいて第１の復号モジュール(16)を選択し、
前記解読されたペイロード(104)を復号するために、前記解読されたペイロード(104)を前記第１の復号モジュール(16)に経路指定するように構成された受信器。
【請求項１０】
ヘッダ(101)と暗号化されたペイロード(102)とを含むデータストリームを処理する受信器(1b)であって、前記ヘッダ(101)は第１のパケット識別子(103)を含み、
前記受信器(1b)は、
前記暗号化されたペイロード(102)を解読して解読されたペイロード(104)を取得するように構成されたデスクランブラ(11)と、
プロセッサ(13b)と、
ルータ(15)と
を備え、
前記プロセッサ(13b)は、
第２のパケット識別子(107)および第１のコンテンツタイプ識別子(108)をハードコードされたメモリ(14b)から取得し、
前記第１のパケット識別子(103)を前記ハードコードされたメモリ(14b)に記憶された前記第２のパケット識別子(107)と比較して第１の比較結果を取得し、
前記第１の比較結果が第１の所定の条件に合致する場合に、前記第１のコンテンツタイ

プ識別子(108)を前記ルータ(15)に供給するように構成され、
前記ルータ(15)は、
前記第１のコンテンツタイプ識別子(108)に基づいて第１の復号モジュール(16)を選択し、
前記解読されたペイロード(104)を復号するために、前記解読されたペイロード(104)を前記第１の復号モジュール(16)に経路指定するように構成された受信器。
【請求項１１】
前記プロセッサ(13a、13b)は、前記第１のコンテンツタイプ識別子(108)に基づいて予め定義された１組のインターフェースからインターフェース(17)を選択し、前記第１の復号モジュール(16)の出力を前記インターフェース(17)に制限するようにさらに構成される、請求項９または請求項１０に記載の受信器(1a、1b)。
【請求項１２】
平文の第３のパケット識別子(109)と、前記第３のパケット識別子(109)に関連付けられた平文の第２のコンテンツタイプ識別子(110)とを受け取るように構成された第２の入力モジュール(18)をさらに備え、
前記プロセッサ(13a、13b)は、
前記第１の比較結果が第２の所定の条件に合致する場合に、前記第１のパケット識別子(103)を前記第３のパケット識別子(109)と比較して第２の比較結果を取得し、
前記第２の比較結果が第３の所定の条件に合致する場合に、前記第２のコンテンツタイプ識別子(110)に基づいて第２の復号モジュール(19)を選択し、かつ、前記解読されたペイロード(104)を復号するために、前記解読されたペイロード(104)を前記第２の復号モジュール(19)に経路指定するようにさらに構成された請求項９から１１のいずれか一項に記載の受信器(1a、1b)。
【請求項１３】
保護されたチップセット(30)をさらに備え、
前記デスクランブラ(11)、前記プロセッサ(13a、13b)、前記メモリ(14a、14b)、前記ルータ(15)、および前記第１の復号モジュール(16)は、前記保護されたチップセット(30)の一部である請求項９から１２のいずれか一項に記載の受信器(1a、1b)。
【請求項１４】
請求項９に記載の受信器(1a)において使用するためのスマートカード(2a)であって、
受信器(1a)から暗号化された第２のパケット識別子(105)と暗号化された第１のコンテンツタイプ識別子(106)とを受け取るように構成された入力モジュール(21)と、
前記暗号化された第２のパケット識別子(105)を解読して第２のパケット識別子(107)を取得し、前記暗号化された第１のコンテンツタイプ識別子(106)を解読して前記第２のパケット識別子(105)に関連付けられた第１のコンテンツタイプ識別子(108)を取得するように構成された解読器(22)と、
安全な接続を通じて前記第２のパケット識別子(107)と前記第１のコンテンツタイプ識別子(108)とを前記受信器(1a)に供給するように構成された出力モジュール(23)と、
を備えるスマートカード。
【請求項１５】
請求項１０に記載の受信器(1b)において使用するためのスマートカード(2b)であって、
第２のパケット識別子(107)と、前記第２のパケット識別子(107)に関連付けられた第１のコンテンツタイプ識別子(108)とを含むハードコードされたメモリ(24)と、
安全な接続を通じて前記第２のパケット識別子(107)と前記第１のコンテンツタイプ識別子(108)とを前記受信器(1b)に供給するように構成された出力モジュール(23)と、
を備えるスマートカード。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、スマートカードに関連しうる、受信器でのデータストリームの安全な解読お

よび復号に関する。
【背景技術】
【０００２】
限定受信(CA)システムでの有料テレビ応用例は、デジタルテレビ放送ストリームを保護するためにスクランブル(暗号化としても知られる)を用いる。受信器を使用し、デジタルテレビストリームを表示する前にストリームをデスクランブルするための関連する解読鍵を得る。このような解読鍵は、制御ワードまたはCWとしても知られる。デジタルテレビ局の中継局では、一続きのCWが音声、映像、サブタイトル、テレテキストおよび/またはアプレットなどの１つまたは複数のエレメンタリストリームに関連付けられる。MPEG2ストリームの場合、エレメンタリストリームはPID(パケット識別子)によって識別される。通常、CWのストリームは、CW_Stream_IDによって識別可能である。MPEG2標準では、テレビサービス(MPEG2用語でのプログラムストリーム)を構成するPIDのリストは、平文のPMT(プログラムマップテーブル)に含まれる。CAシステムは、CW_Stream_IDをいくつかのPIDにマッピングするために同様なデータ構造を使用する。受信器内のデコーダは、PMTを処理し、CAシステムのスマートカードは、CW_Stream_IDを関連するPIDに結び付ける情報を処理し、エレメンタリストリームをデスクランブルために関連する鍵をロードするように受信器をセットアップする。
【０００３】
平文のデジタルテレビストリームへの無許可アクセスを防止するために、通常は安全なチップまたはチップセット内の、受信器の保護領域内でデジタルテレビ信号のデスクランブルおよび復号を実施することが知られている。
【０００４】
知られている受信器は通常、MPEG2ストリームの処理において以下のステップをとる。MPEG2パケットは受信され、復調される。MPEG2ヘッダからPIDおよびスクランブル制御フィールドが抽出される。受信器のメモリ内のCWルックアップテーブル内で一致するPID値を有する項目が検索され、関連付けられたCW鍵がテーブルから読み出される。関連付けられたCW鍵から、デスクランブラにロードする必要があるCWを選択するために、スクランブル制御フィールド値が用いられる。スクランブルされたMPEG2パケットのペイロードは、CWを用いてデスクランブラにおいて解読される。平文のMPEG2 PMTからの情報は、パケットのstream_typeを判定するために用いられる。stream_typeは、例えば音声、映像、サブタイトル、テレテキストまたはアプレットなどのコンテンツのタイプを識別するコンテンツタイプ識別子である。stream_typeは、パケットを適切な復号モジュールに送るために用いられる。
【０００５】
MPEG2ストリームを処理するために受信器は、通常、次の入力、すなわちMPEG2パケットヘッダからのPID値およびスクランブル制御フィールドと、平文のMPEG2 PMT情報、そのうち特にエレメンタリストリームのPIDおよびPIDに関連付けられたstream_typeを用いる。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
受信器の意図された動作を確実にするために、これらすべての入力データは正確な情報を供給することが必要である。PMTおよびMPEG2パケットヘッダは平文にて供給されるので、これらは受信器内で処理される前に改竄され得る。これは攻撃者がPID値またはstream_type値を変更して、例えば映像および音声エレメンタリストリームをテレテキストストリームのように見せることを可能にする。映像ストリームおよび音声ストリームは、通常、受信器の保護された領域内で処理され、一方、デスクランブルの後にはテレテキストストリームは保護された領域の外側で処理される。したがって入力のこのような改竄は、デスクランブルされた映像および音声エレメンタリストリームを保護領域から出させ、これらのストリームへの無許可アクセスを可能にし、ストリームの処理を信頼できないものにする。

【課題を解決するための手段】
【０００７】
本発明の目的は、データストリームの安全な処理を向上することである。
【０００８】
本発明の一態様によれば、受信器においてデータストリームを処理する方法が提案される。データストリームは、ヘッダと、暗号化されたペイロードとを含む。ヘッダは、第１のパケット識別子を含む。この方法は、暗号化されたペイロードを解読して解読されたペイロードを取得するステップを含む。この方法はさらに、暗号化された第２のパケット識別子と、暗号化された第１のコンテンツタイプ識別子とを受け取るステップを含む。この方法はさらに、保護された環境内で、暗号化された第２のパケット識別子から第２のパケット識別子を取得するステップを含む。この方法はさらに、保護された環境内で、第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を、暗号化された第１のコンテンツタイプ識別子から取得するステップを含む。この方法はさらに、第１のパケット識別子を第２の識別子と比較して第１の比較結果を取得するステップを含む。この方法はさらに、第１の比較結果が第１の所定の条件に合致する場合に、第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択するステップと、解読されたペイロードを復号するために、解読されたペイロードを第１の復号モジュールへ経路指定するステップとを含む。
【０００９】
本発明の一態様によれば、データストリームを処理するための受信器が提案される。データストリームは、ヘッダと、暗号化されたペイロードとを含む。ヘッダは、第１のパケット識別子を含む。この受信器は、暗号化されたペイロードを解読して解読されたペイロードを取得するように構成されたデスクランブラを備える。この受信器はさらに暗号化された第２のパケット識別子と、暗号化された第１のコンテンツタイプ識別子とを受け取るように構成された第１の入力モジュールを備える。この受信器はさらに、プロセッサと、メモリと、ルータとを備える。このプロセッサは、暗号化された第２のパケット識別子から第２のパケット識別子を取得するように構成される。このプロセッサはさらに、第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を、暗号化された第１のコンテンツタイプ識別子から取得するように構成される。このプロセッサはさらに、第２のパケット識別子および第１のコンテンツタイプ識別子をメモリに記憶するように構成される。このプロセッサはさらに、第１のパケット識別子をメモリに記憶された第２のパケット識別子と比較して第１の比較結果を取得するように構成される。このプロセッサはさらに、第１の比較結果が第１の所定の条件に合致する場合に、第１のコンテンツタイプ識別子をルータに供給するように構成される。このルータは、第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択するように構成される。このルータはさらに、解読されたペイロードを復号するために、解読されたペイロードを第１の復号モジュールへ経路指定するように構成される。
【００１０】
第１の所定の条件は、例えば第１のパケット識別子が第２のパケット識別子と等しいことである。
【００１１】
したがって、第１のコンテンツタイプ識別子、および関連付けられた第２のパケット識別子は、処理のために安全に受信器に供給され、すなわち暗号化されしたがって改竄不可能な形で受け取られる。さらに、解読されたペイロードの処理は、改竄不可能な第１のコンテンツタイプ識別子に依存する。好ましくは、これは受信器内で処理される前にコンテンツタイプ識別子を変更するのを大幅に複雑化する。
【００１２】
好ましくは請求項２の実施形態は、第１のコンテンツタイプ識別子の保護された分配のために、エンタイトルメント制御メッセージおよび/またはエンタイトルメント管理メッセージの使用を可能にする。

【００１３】
本発明の一態様によれば、受信器においてデータストリームを処理する方法が提案される。データストリームは、ヘッダと、暗号化されたペイロードとを含む。ヘッダは、第１のパケット識別子を含む。この方法は、保護された環境内で、暗号化されたペイロードを解読して解読されたペイロードを取得するステップを含む。この方法はさらに、保護された環境内で、ハードコードされたメモリから第２のパケット識別子を取得するステップを含む。この方法はさらに、ハードコードされたメモリから第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を取得するステップを含む。この方法はさらに、第１のパケット識別子を第２の識別子と比較して第１の比較結果を取得するステップを含む。方法はさらに、第１の比較結果が第１の所定の条件に合致する場合に、第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択するステップと、解読されたペイロードを復号するために、解読されたペイロードを第１の復号モジュールへ経路指定するステップとを含む。
【００１４】
本発明の一態様によれば、データストリームを処理する受信器が提案される。データストリームは、ヘッダと、暗号化されたペイロードとを含む。ヘッダは、第１のパケット識別子を含む。この受信器は、暗号化されたペイロードを解読して解読されたペイロードを取得するように構成されたデスクランブラを備える。この受信器はさらに、プロセッサと、ルータとを備える。このプロセッサは、ハードコードされたメモリから第２のパケット識別子、および第１のコンテンツタイプ識別子を取得するように構成される。このプロセッサはさらに、第１のパケット識別子をハードコードされたメモリに記憶された第２のパケット識別子と比較して第１の比較結果を取得するように構成される。このプロセッサはさらに、第１の比較結果が第１の所定の条件に合致する場合に、第１のコンテンツタイプ識別子をルータに供給するように構成される。このルータは、第１のコンテンツタイプ識別子に基づいて第１の復号モジュールを選択するように構成される。このルータはさらに、解読されたペイロードを復号するために、解読されたペイロードを第１の復号モジュールへ経路指定するように構成される。
【００１５】
第１の所定の条件は、例えば第１のパケット識別子が第２のパケット識別子と等しいことである。
【００１６】
したがって、第１のコンテンツタイプ識別子、および関連付けられた第２のパケット識別子は、処理のために安全に受信器に供給され、すなわちハードコードされたメモリから、したがって改竄不可能な形で得られる。さらに、解読されたペイロードの処理は、改竄不可能な第１のコンテンツタイプ識別子に依存する。好ましくは、これは受信器内で処理される前にコンテンツタイプ識別子を変更することを不可能にする。
【００１７】
好ましくは請求項４の実施形態は、受信器内のハードコードされたメモリを使用可能にする。
【００１８】
好ましくは請求項５の実施形態は、スマートカード内のハードコードされたメモリを使用可能にする。
【００１９】
好ましくは請求項６および１１の実施形態は、デコーダの出力を、例えばHDMI/HDCPインターフェース、DVI/HDCPインターフェース、またはDRM保護インターフェースなどの予め定義されたインターフェースに制限することを可能にする。HDMI、HDCP、DVI、およびDRMは、それぞれHigh-Definition Multimedia Interface、High-Bandwidth Digital Content Protection、Digital Visual Interface、およびDigital Rights Managementの知られている略語である。
【００２０】

好ましくは請求項７および１２の実施形態は、無許可アクセスが可能となり得る解読されたペイロードの安全性の低い処理を可能にする。第２の所定の条件は、例えば第１のパケット識別子が第２のパケット識別子と異なることである。第３の所定の条件は、例えば第１のパケット識別子が第３のパケット識別子と等しいことである。

【００２１】

好ましくは請求項８の実施形態は、MPEG2ストリームの安全で改竄不可能な処理を可能にする。

【００２２】

好ましくは請求項１３の実施形態は、受信器内の信号の盗聴を防止する。

【００２３】

本発明の一態様によれば、上述の特徴の１つまたは複数を有する受信器内で使用するためのスマートカードが提案される。このスマートカードは、受信器から暗号化された第２のパケット識別子と、暗号化された第１のコンテンツタイプ識別子とを受け取るように構成された入力モジュールを備える。このスマートカードはさらに、暗号化された第２のパケット識別子を解読して第２のパケット識別子を取得し、暗号化された第１のコンテンツタイプ識別子を解読して第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を取得するように構成された解読器を備える。このスマートカードはさらに、第２のパケット識別子および第１のコンテンツタイプ識別子を受信器に供給するように構成された出力モジュールを備える。

【００２４】

したがって好ましくはこのスマートカードは、第２のパケット識別子および第１のコンテンツタイプ識別子を安全に取得し、これらを安全に受信器に供給するために用いることができる。

【００２５】

本発明の一態様によれば、上述の特徴の１つまたは複数を有する受信器内で使用するためのスマートカードが提案される。このスマートカードは、ハードコードされたメモリを備える。ハードコードされたメモリは、第２のパケット識別子、および第２のパケット識別子に関連付けられた第１のコンテンツタイプ識別子を含む。このスマートカードはさらに、第２のパケット識別子および第１のコンテンツタイプ識別子を受信器に供給するように構成された出力モジュールを備える。

【００２６】

したがって好ましくはこのスマートカードは、第２のパケット識別子および第１のコンテンツタイプ識別子を安全に取得し、これらを安全に受信器に供給するために用いることができる。

【００２７】

本明細書では以下に、本発明の実施形態についてさらに詳しく説明する。しかし、これらの実施形態は、本発明に対する保護の範囲を限定するものと解釈することはできないことを理解されたい。

【００２８】

本発明の態様について、図面に示された例示的実施形態を参照することによって、より詳しく説明する。

【図面の簡単な説明】

【００２９】

【図１ａ】本発明の例示的実施形態の受信器を示す図である。

【図１ｂ】本発明の例示的実施形態の受信器を示す図である。

【図２ａ】本発明の例示的実施形態のスマートカードを示す図である。

【図２ｂ】本発明の例示的実施形態のスマートカードを示す図である。

【図３】本発明の例示的実施形態の受信器およびスマートカードでのデータフローを示す図である。

【図４ａ】本発明の例示的実施形態の受信器において実行される方法のステップの概略図

である。
【図４ｂ】本発明の例示的実施形態の受信器において実行される方法のステップの概略図である。
【図５】本発明の例示的実施形態の受信器において実行される方法のステップの概略図である。
【発明を実施するための形態】
【００３０】
CAシステムでは受信器は、暗号化されたデータパケットがそれから抽出され処理される、データストリームを受け取るデバイスである。データストリームは、放送ストリームとして受け取ることができ、または例えばハードディスクまたはDVDディスク上に記憶されたファイルから生じ得る。データパケットは、ヘッダと暗号化されたペイロードとを有する。受信器では、暗号化されたペイロードは、テレビジョン、PC、または音声再生デバイスなどのエンドユーザデバイス上での再生を可能にするために解読され、復号される。コンテンツのタイプに応じて、特定のデコーダが用いられる。コンテンツのタイプは、例えば音声、映像、サブタイトル、テレテキストおよびアプレットである。一部のタイプのコンテンツは、映像および音声ストリームなど、その高価な特質のためにハッカーにとって特に興味がある。
【００３１】
データストリームは、例えばISO 13818-1標準に適合するMPEG2ストリームである。MPEG2ストリームは、通常、ヘッダとペイロードを有するデータパケットをそれぞれが含む複数のエレメンタリストリームを含む。ヘッダは、パケット識別子(PID)を含む。ペイロードは、特定のコンテンツタイプに属するコンテンツを含む。MPEG2標準によりPMTは、平文にて、場合によりペイロード内のデータ構造体として、別に受信器に供給される。PMTは、PIDをstream_typeと呼ばれるコンテンツタイプ識別子に結び付ける情報を含む。エレメンタリストリーム内で受け取られたPIDを、PMT内で受け取られたPIDと比較することにより、ペイロードのstream_typeを検出することが可能である。PMTの特性が平文であることにより、ハッカーにより改竄可能となる。
【００３２】
本発明は、入力データを安全に受信器に供給することによって、このような改竄に対する保護をもたらす。入力データは、中でも識別可能なペイロードに対するコンテンツタイプ識別子を含む。入力データは、それが改竄から保護される受信器内で用いられる。ここで入力データは、放送ストリーム内で暗号化されているか、あるいはメモリ内でハードコード(hardcode)される。入力データを得るためにスマートカードが用いられる場合は、既存の技術を用いて受信器とスマートカードの間で安全にデータを交換することができる。受信器内では、ペイロードおよび入力データは、好ましくはデータ信号が盗聴できないことを確実にする保護されたチップ、または保護されたチップセット内で処理される。
【００３３】
図１ａには、受信器1aが示される。第１の入力モジュール12を通じて、入力データは安全に受け取られる。受け取られた入力データは暗号化されており、PIDと、PIDに関連付けられたstream_typeとを含む。プロセッサ13aは、例えば受信器1a内で入力データを解読することにより、またはスマートカードによって入力データを解読させることにより、入力データからPIDとstream_typeとを取得する。取得されたPIDとstream_typeは、後に参照するためにメモリ14aに記憶される。複数のPIDおよび関連するstream_typeを取得し、メモリ14aに記憶することができる。メモリ14aでのより効率的な記憶を可能にするために、stream_typeに関連する一連のPIDをもつことができる。
【００３４】
受信器1aはさらに、データパケットの暗号化されたペイロードを解読するためのデスクランブラ11を含む。暗号化されたペイロードは、例えばMPEG2エレメンタリストリームから、またはファイルから生じる。データパケットは、ペイロードを識別するPIDを含むヘッダを有する。暗号化されたペイロードを解読した後に、解読されたペイロードは、特定

のデコーダによって復号されることになる。デコーダは、データパケットのヘッダからのPIDをメモリ14aに記憶されたPIDと比較することによって選択される。一致が検出された場合は、関連付けられたstream_typeがメモリから読み出され、対応する復号モジュール16が選択される。stream_typeは、例えば用いられるべき復号モジュール16を示すものであり、またはstream_typeは、対応する復号モジュール16を検出するためのテーブル内のルックアップを可能にする。stream_typeを用いて復号モジュール16を検出するために、任意の他の機構を用いることができる。ルータ15は、解読されたペイロードを選択された復号モジュール16に経路指定し、解読されたペイロードはそこで復号することができる。

【００３５】

図１ｂには、代替の受信器1bが示される。受信器1bでは、PIDおよび関連するstream_typeはメモリ14bにハードコードされ、したがって受信器1a内の入力モジュール12のような入力モジュールを通じて供給する必要はない。入力モジュール12を通じた入力データの安全な受け取りを別として、受信器1bは受信器1aと同様に動作する。図１ｂでメモリ14bは、受信器1bの内部にある。代替としてメモリ14bは、受信器1bによってアクセス可能なスマートカード内に設けることもできる。

【００３６】

図２ａには、PIDおよび関連するstream_typeを得るために図１ａに示される受信器1aと共に用いることができるスマートカード2aが示される。入力モジュール21は、暗号化されたPIDと暗号化されたstream_typeとを含む暗号化された入力データを受信器から受け取る。解読器22は入力データを解読し、それにより得られた解読されたPIDとstream_typeは、出力モジュール23を通じて受信器1aに供給される。スマートカード2aと受信器1aの間のインターフェースは、任意の知られているスマートカードインターフェース技術を用いて保護される。

【００３７】

図２ｂは、PIDおよび関連するstream_typeを得るために図１ｂに示される受信器1bと共に用いることができる代替のスマートカード2bを示す。PIDおよび関連するstream_typeは、ハードコードされたメモリ24に記憶され、出力モジュール23を通じて受信器1bに供給される。

【００３８】

図３には、本発明の例示的実施形態の受信器においてどのようにデータが処理されるかがより詳しく示される。簡単にするためにプロセッサ13a、13bは示していない。データフローは破線の矢印によって示される。コンマによって分けられる参照番号は、代替を示す。セミコロンによって分けられる参照番号は、要素間の複数のデータフローを示す。メモリ14a、14bは、ハードコードされたメモリ14bである場合にはスマートカード2a、2bは用いられず、または、メモリ14aである場合にはスマートカード2a、2bが用いられて、スマートカード2a内の暗号化された入力データからPIDおよび関連するstream_typeを取得し、またはスマートカード2b内のハードコードされたメモリ24からPIDおよび関連するstream_typeを取得する。

【００３９】

メモリ14a、14bには、PIDおよび関連するstream_typeが記憶される。さらに、PIDおよび関連するCWが記憶される。CWは、例えば予め定義された時間フレームに対して２つのCWがPIDに関連付けられるエンタイトルメント制御メッセージ(ECM)など、それ自体は知られている方法で受信器内で受け取られる。２つのCWは、奇CW(odd CW)および偶CW(even CW)と呼ばれ、暗号化されたペイロードを含むデータパケットのヘッダ内のスクランブル制御フィールドを用いて選択することができる。PID、stream_type、およびCWがどのように記憶されるかの一実施例は、以下の表に示され、これは信頼できる情報ルックアップテーブルとして用いることができる。stream_typeをPIDに関連付けることができ、CWをPIDに関連付けることができるならば、これらのデータを記憶するための他の任意の構造を用いることができる。

【００４０】

【表１】

信頼できる情報ルックアップテーブル			
PID	CW_odd	CW_even	Stream_type
101	CW1	CW2	映像
201-299	CW3	CW4	l
$\{\delta_{100}\} \geq 0$	CW1	CW2	音声

【００４１】

信頼できる情報ルックアップテーブルは、データを有する３つの行を含む。第１の行では、"101"の値を有するPID、"CW1"の値を有する奇CW、"CW2"の値を有する偶CW、および"映像"の値を有するstream_typeが記憶される。したがってCW1とCW2はPID101に関連付けられ、PID101は、映像というstream_typeに関連付けられる。第２の行では、一連のPID201～299がCW3、CW4、および1のstream_typeに関連付けられ、stream_typeの値1は例えば映像を表す。第３の行では、一連のPID

【００４２】

【数１】

$$\{\delta_{100}\} \geq 0$$

【００４３】

、すなわち{0，100，200，...}がCW1、CW2、および音声というstream_typeに関連付けられる。

【００４４】

図３を参照すると、以下の実施例では、PIDおよび関連するCWはECM内で受け取られ、PIDおよび関連するstream_typeはエンタイトルメント管理メッセージ(EMM)内で受け取られる。ECMおよびEMMは、受信器1aの保護された領域30内の第１の入力モジュール12によって受け取られ、受信器1aとスマートカード2aの間の安全なインターフェースを通じてスマートカード2aに転送される。暗号化された奇CW112aおよび暗号化された偶CW112bはスマートカード2a内で解読され、解読された奇CW113aおよび解読された偶CW113bとして、ECMからのPID情報と共に、安全なインターフェースを通じて受信器1aに供給され、そこでそれらはメモリ14aに記憶される。暗号化されたPID105および暗号化されたstream_type106もスマートカード2a内で解読され、解読されたPID107および解読されたstream_type108として受信器1aに供給され、そこでそれらはメモリ14aに記憶される。MPEG2エレメンタリストリームが受け取られたときは、エレメンタリストリームのヘッダ101からデータフィールドが抽出され、エレメンタリの暗号化されたペイロード102がデスクランブラ11に供給される。ヘッダから抽出されたデータフィールドの中には、ペイロードを識別するPID103と、暗号化されたペイロードを解読するために奇CWが用いられるべきか偶CWが用いられるべきかを識別するスクランブル制御フィールド111とがある。

【００４５】

PID103に対するCW113a;113bは、メモリ14a内で検索され、スクランブル制御フィールド111の値に基づいてスイッチ10は、奇CW113aまたは偶CW113bのいずれかをデスクランブラ11に供給する。デスクランブラ11は、供給された奇CW113aまたは偶CW113bを用いて暗号化されたペイロード102を解読する。ペイロードを解読した後に、stream_type108が、解読されたペイロード104と共にルータモジュール15に送られる。ルータモジュール15は、メモリ14aに記憶された信頼できる情報ルックアップテーブルからのstream_type108を用いて、解読されたペイロード104を復号するために適切なデコーダを選択する。したがって従来技術とは対照的に、平文のPMTにて供給され第２の入力モジュール18を通じて受け取られるPID109およびstream_type110の情報は使用されない。stream_typeが空(nil)である、すなわちメモリ14a内では得られない、または無効の場合は、ルータはPMTからの情報を

用いるように構成することができる。第２の入力モジュール18と第１の入力モジュール12は、同じ１つとすることができる。

【００４６】

保護された領域30内のstream_type108は、復号モジュール16のための関連する経路指定情報を含むまたは有することができる。これにより例えばプレミアムなコンテンツの送信は、SCARTおよびS-videoなどの保護されない高品質アナログインターフェース上ではなく、HDMIなどの保護された出力インターフェース17に制限することが可能になる。

【００４７】

信頼できるstream_typeのロードおよび供給を実施するにはいくつかの方法がある。CAシステムは、通常、PID値をCW_Stream_IDによって参照されるCWのストリームに関連付ける機構を用意する。この機構は、いくつかのエレメンタリストリームがCW値を共有することを可能にする。CW_Stream_IDのPID値への関連付けは、そのCW_Stream_IDに対する一続きのCWの送信の前に生じる。したがってECMは、少なくともCW_Stream_IDと、CW112a、112bの暗号化されたバージョンを含む。CW_Stream_IDに対するPIDのリストは、追加の信頼できるstream_type107に対する良好な基準をもたらす。そのときは単一のPID値の代わりに、CW_Stream_IDの関連付けは、{PID107、stream_type108}の対の配列からなる。CW_Stream_IDの関連付けのリストを処理した後に、スマートカード1aは、安全な情報ロードプロトコルを用いて、信頼できるstream_type108を受信器1aの保護された領域30に送信することができる。

【００４８】

別法として、いくつかのPID値107に対する信頼できるstream_type108を含む、特別なデータストリームが定義される。データへの変更を防止するために、この特別なデータストリームは暗号化される。特別なデータストリームは、受信器の保護された領域30内のデスクランブラ、場合によりデスクランブラ11にて解読される。PID107とstream_type108の間の関連付けは構文解析され、保護された領域30で用いるためにメモリ14aに記憶される。

【００４９】

別法として、CWをロードするために２つの別々のCWルックアップテーブル、および別々の鍵ラダー(key ladder)が生成される。この目的には、知られている鍵ラダーモジュールを用いることができる。一方のCWルックアップテーブルは、保護された領域30内に留まる必要があるストリームに対する情報を含み、他方のCWルックアップテーブルは、保護された領域30の外側のデコーダ19によって復号することが許されるエレメンタリストリームを扱う。この目的には、1の値または0の値を有する2値のstream_typeを用いることができる。鍵ラダーモジュールは、チップのワンタイムプログラマブルメモリ構造に埋め込まれた簡単な鍵階層を用いて、CW113a、113bをチップの保護された領域30内に直接ロードするように安全なセッション処理を実施する。

【００５０】

受信器1aへのCWおよびstream_typeの供給のために、他の代替方法を用いることもできる。

【００５１】

図４ａは、本発明の例示的実施形態の受信器、例えば図１ａに示される受信器で行われる方法のステップを示す。好ましくはステップは、受信器1aの保護されたチップ30内で行われる。ステップ1001では、暗号化された映像ペイロードなどの、エレメンタリストリームの暗号化されたペイロード102は解読されて、解読された映像104となる。ステップ1002ではECMまたはEMMが、暗号化されたPID105および暗号化されたstream_type106と共に受け取られる。PID105はステップ1003で解読され、メモリ14aに記憶され、stream_type106はステップ1004で解読され、メモリ14aに記憶される。解読されたPID107は、ステップ1005で映像ペイロードのPID103と比較される。ここでPID103はエレメンタリストリームのヘッダから抽出され、メモリ14aに記憶されたPIDと比較される。一致が検出された場合は、これはステップ1006によって示され、PID103(または、この場合は同一であるPID107)に関連付けられたstream_type108がメモリ14aから読み出され、ステップ1007で映像ペイロード

を復号するために映像復号モジュール16を選択するために用いられる。ステップ1008では、解読された映像ペイロードは、映像復号モジュール16に経路指定される。

【００５２】

図４ｂは、本発明の例示的実施形態の受信器、例えば図１ｂに示される受信器で行われる代替方法のステップを示す。方法は、PID107および関連するstream_type108を得るためにECMまたはEMMを受け取る代わりに、PID107およびstream_type109はメモリ内、例えば受信器1bのハードコードされたメモリ14b内、またはスマートカード2bのハードコードされたメモリ24内にハードコードされるという点で図１ａと異なる。ステップ1011では、ハードコードされたメモリ14bまたは24からPID107が読み出され、ステップ1012では、ハードコードされたメモリ14bまたは24からstream_typeが読み出される。

【００５３】

図５には、本発明の例示的実施形態の受信器、例えば図１ａに示される受信器で行われる方法の追加的なオプションのステップが示される。図４ａに示されるステップに加えて図５の例示的実施形態では、ステップ1013でインターフェース17が選択されて、ステップ1014でデコーダ16の出力を制限する。stream_typeがメモリ14a内で検出されない場合に受信器1aは、受信器にて安全性なく受け取られた入力データに基づいて、この場合は例えばテレテキストペイロードである解読されたペイロード104を経路指定するように構成することができる。平文のPID109と、PID109に関連付けられた平文のstream_type110とを含む入力データは、例えばPMT内で受け取られる。ステップ1015では、PMTが受け取られる。ステップ1016ではPMTからのPID109は、テレテキストペイロード104のPID103と比較される。PIDが一致する場合は、これはステップ1017で示され、受信器の保護された領域30の外側のテレテキスト復号モジュール19がステップ1018で選択される。ステップ1019ではテレテキストペイロード104は、テレテキスト復号ユニット19へ経路指定される。

【００５４】

図５に示される追加的なオプションのステップは、図４ｂの実施例にも同様に適用することができる。

【００５５】

本発明の一実施形態は、コンピュータシステムと共に用いるためのプログラム製品として実施することができる。プログラム製品のプログラムは、実施形態の機能(本明細書で述べた方法を含む)を定義し、様々なコンピュータ読み取り可能な記憶媒体上に含むことができる。例示的なコンピュータ読み取り可能な記憶媒体は非限定的に、(i)情報が永久的に記憶される非書き込み可能記憶媒体(例えばCD-ROMドライブによって読み出し可能なCD-ROMディスク、フラッシュメモリ、ROMチップ、または任意のタイプの固体不揮発性半導体メモリなどの、コンピュータ内のリードオンリメモリデバイス)、および(ii)変更可能な情報が記憶される書き込み可能記憶媒体(例えばディスケットドライブ内のフロッピー(登録商標)ディスク、ハードディスクドライブ、または任意のタイプの固体ランダムアクセス半導体メモリ)を含む。

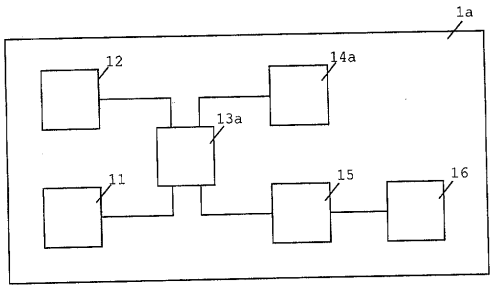
【符号の説明】

【００５６】

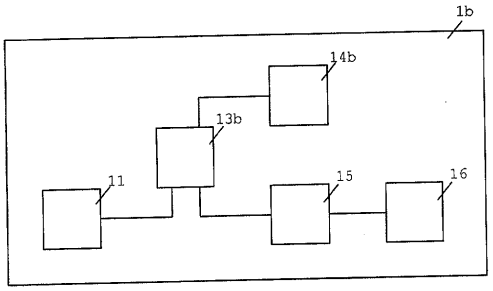
1a、1b　受信器
2a、2b　スマートカード
10　スイッチ
11　デスクランブラ
12　第１の入力モジュール
13a　プロセッサ
13b　プロセッサ
14a　メモリ
14b　ハードコードされたメモリ
15　ルータ
16　第１の復号モジュール

17　インターフェース
18　第２の入力モジュール
19　第２の復号モジュール
21　入力モジュール
22　解読器
23　出力モジュール
24　ハードコードされたメモリ
30　保護された領域
101　ヘッダ
102　暗号化されたペイロード
103　第１のパケット識別子
104　解読されたペイロード
105　第２のパケット識別子
106　暗号化された第１のコンテンツタイプ識別子
107　第２のパケット識別子
108　第１のコンテンツタイプ識別子
109　第３のパケット識別子
110　第２のコンテンツタイプ識別子
111　スクランブル制御フィールド
112a　暗号化された奇CW
112b　暗号化された偶CW
113a　解読された奇CW
113b　解読された偶CW

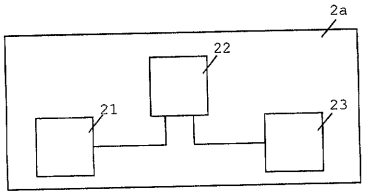
【図１ａ】



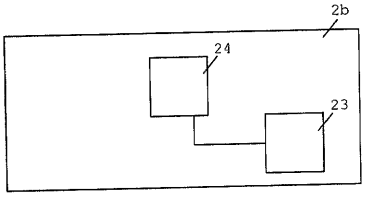
【図１ｂ】



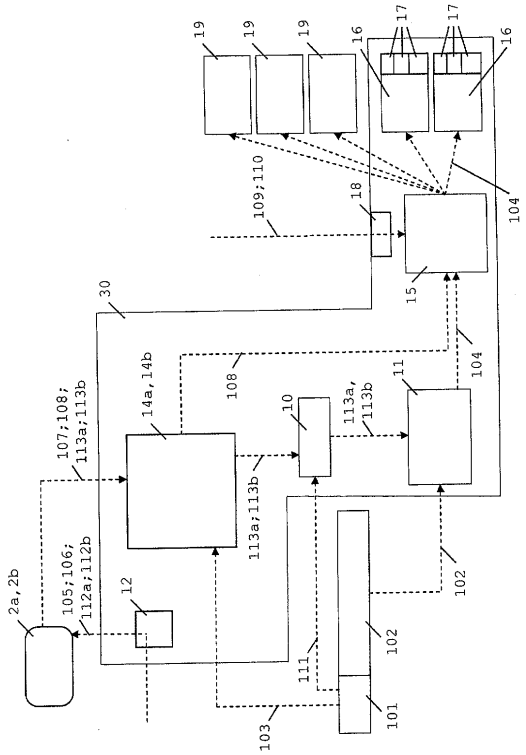
【図２ａ】



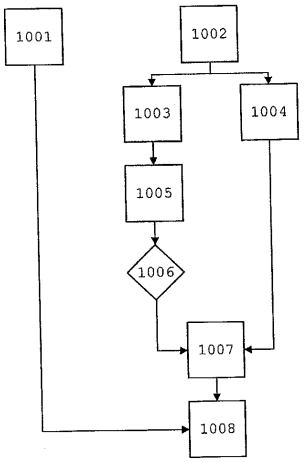
【図２ｂ】



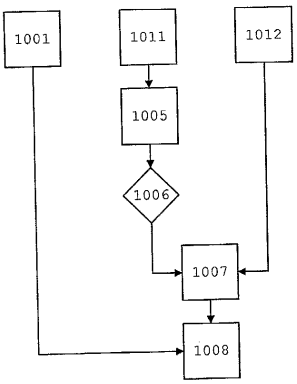
【図３】


19
19
19
16
17
17
16
109;110
18
104
30
15
104
108
14a,14b
11
10
113a,
113b
107;108;
113a;113b
113a;113b
105;106;
112a;112b
12
2a,2b
102
102
111
101
103

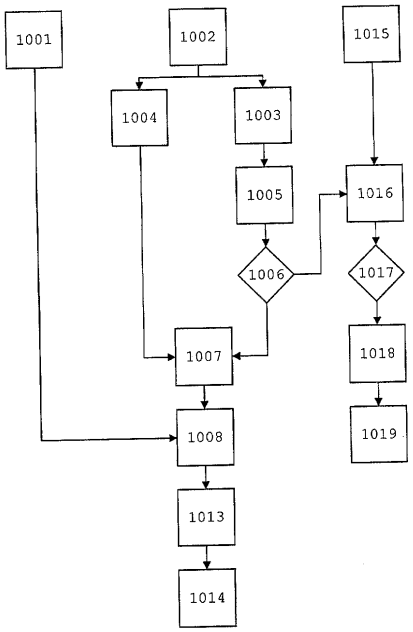
【図４ａ】


1001
1002
1003
1004
1005
1006
1007
1008

【図４ｂ】


1001
1011
1012
1005
1006
1007
1008

【図５】


1001
1002
1015
1004
1003
1005
1016
1006
1017
1007
1018
1008
1019
1013
1014

フロントページの続き

(72)発明者　アルナウト・エフェルト・ファン・フォレースト
オランダ・２３１２・ウェー・エス・ライデン・フラウウェンケルクシュテーク・１３
(72)発明者　ヨハン・ヘラルト・デケール
オランダ・２５１２・エーベー・ニーウーフェンネプ・ラーン・ファン・ルーフェスタイン・３０
(72)発明者　ブルース・フィクトル・クルティン
オランダ・２０２４・イクスベー・ハールレム・ミデンヴェーク・１０９

審査官　岩井　健二

(56)参考文献　特開２００８－１１３１０４（ＪＰ，Ａ）
特開２００７－０９６８９６（ＪＰ，Ａ）
特開２００４－１７３０７９（ＪＰ，Ａ）
特開２００３－０６９９７４（ＪＰ，Ａ）
特開２０００－０１３６９６（ＪＰ，Ａ）
特開平０９－０５１５２０（ＪＰ，Ａ）
米国特許出願公開第２００７／０２６３８６４（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１４８５０１（ＵＳ，Ａ１）
欧州特許出願公開第１８１９０７５（ＥＰ，Ａ２）
欧州特許出願公開第１３９２０６０（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ　２１／００　－　２１／８５８
Ｈ０４Ｌ　９／３６