(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-515885
(P2007-515885A)
(43)公表日　平成19年6月14日(2007.6.14)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	7/173	(2006.01)	H04N	7/173	610Z	5C164
H04L	9/14	(2006.01)	H04N	7/173	630	5J104
			H04L	9/00	641	

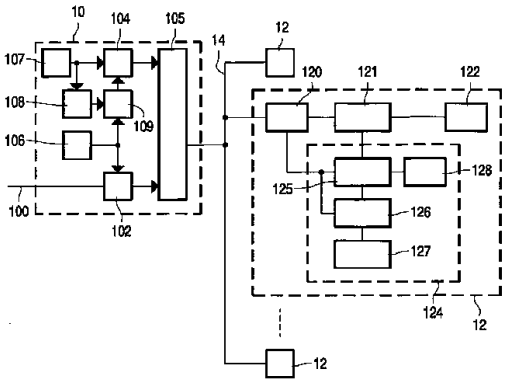
審査請求 未請求　予備審査請求 未請求　（全 19 頁）

(21)出願番号	特願2006-543694 (P2006-543694)
(86)(22)出願日	平成16年12月8日 (2004.12.8)
(85)翻訳文提出日	平成18年6月9日 (2006.6.9)
(86)国際出願番号	PCT/IB2004/052705
(87)国際公開番号	WO2005/057926
(87)国際公開日	平成17年6月23日 (2005.6.23)
(31)優先権主張番号	03104616.2
(32)優先日	平成15年12月10日 (2003.12.10)
(33)優先権主張国	欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　マイイェン，マリニュス　セー　エム
オランダ国，５６５６　アーアー　アインドーフェン，プロフ・ホルストラーン　６
最終頁に続く

(54)【発明の名称】条件付きアクセス映像信号分配装置及び方法

(57)【要約】
映像信号分配システムは、暗号化映像信号と、映像信号を復号化するためのコントロールワード情報と、映像信号のそれぞれの一部を視聴するための料金を表す料金情報とを有するデータストリームを生成する映像ストリームソース（１０）を有する。複数の映像再生装置（１２）はデータストリームを受信するように媒体（１４）に結合されている。映像再生装置（１２）の各々は、映像信号復号化装置（１２１）にコントロールワード情報から導出されるコントロールワードを供給するためのコントロールワード導出ユニット（１２５）を有する。クレジットメモリ（１２８）を有するクレジット管理ユニットが備えられ、それは、クレジットメモリ（１２８）がクレジットの閾値の金額以上の利用可能性を有するときにコントロールワードの供給をイネーブル又はディセーブルにし、コントロールワードが供給される復号化のための映像信号の一部についての料金情報に従ってクレジットメモリ（１２８）におけるクレジットの金額を低額する。



【特許請求の範囲】
【請求項１】
映像信号分配システムであって：
映像ストリームを生成し且つ媒体に前記映像ストリームを送信するように備えられている映像ストリームソースであって、前記映像ストリームソースは、前記データストリームにおいて、暗号化映像信号と、前記映像信号を復号化するためのコントロールワード情報と、前記映像信号のそれぞれの部分を視聴するための料金を表す料金情報と、を有するように備えられている、映像ストリームソース；並びに
前記媒体に結合されている複数の映像再生装置であって、前記映像再生装置の各々は、前記媒体に結合されている入力及びコントロールワード出力を有する制御ワード供給ユニットであって、制御ワード情報からもたらされるコントロールワードを供給するように備えられている、制御ワード供給ユニットと、
前記媒体に結合されている映像入力と前記コントロールワード出力に結合されているコントロールワード入力とを有する映像信号復号化装置であって、前記コントロールワードを用いて前記映像情報を復号化するように備えられている、映像信号復号化装置と、
クレジットメモリを有するクレジット管理ユニットであって、前記クレジットメモリがクレジットの閾値以上の利用可能性を示すかどうかに依存して、前記コントロールワードの供給をイネーブルに又はディセーブルにコントロール情報をすることを可能にすることを与え、そして前記コントロールワードが供給される復号化のために前記映像信号の一部についての料金情報に従って前記クレジットメモリにおけるクレジットの金額を減額するように、備えられているクレジット管理ユニットと、
を有する、映像再生装置；
を有することを特徴とする映像信号分配システム。
【請求項２】
請求項１に記載の映像信号分配システムであって、前記映像再生装置の各々の前記コントロールワード供給ユニットは、関係する前記映像再生装置において秘密情報へのアクセスを有し、前記映像ストリームソースは、前記映像再生装置の全てに対してアクセス可能であるように前記ストリームにおいて鍵情報を挿入するように備えられ、各々の映像再生装置における前記コントロールワード供給ユニットは、前記鍵情報及び前記秘密情報の一部からコントロールワード復号化鍵を生成する且つ前記コントロールワードを復号化するために前記コントロールワード復号化鍵を用いるように備えられている、ことを特徴とする映像信号分配システム。
【請求項３】
請求項２に記載の映像信号分配システムであって、前記映像ストリームソースは、前記暗号化映像信号間の前記データストリームにおいて暗号化コントロールメッセージを挿入するように備えられ、前記暗号化コントロールメッセージの少なくとも一部は暗号化コントロールワード及び前記鍵情報の両方を有する、ことを特徴とする映像信号分配システム。
【請求項４】
請求項３に記載の映像信号分配システムであって、前記秘密情報と共に前記暗号化コントロールメッセージの特定の一において含まれる前記鍵情報は、前記暗号化コントロールメッセージの特定の一において前記暗号化コントロールワード情報を復号化するように機能する、ことを特徴とする映像信号分配システム。
【請求項５】
請求項２に記載の映像信号分配システムであって、前記ストリームは、前記暗号化コントロールワードのそれぞれの一と前記料金情報の少なくとも一部とを有する暗号化コントロールメッセージを有し、前記コントロールワード供給ユニットは、前記暗号化コントロールメッセージのそれぞれ一からの復号化されたコントロールワードの供給と共に前記暗号化コントロールメッセージのそれぞれの一における前記料金情報に従って前記クレジットの料金を減額するように備えられている、ことを特徴とする映像信号分配システム。

【請求項６】
請求項１に記載の映像信号分配システムであって、前記コントロールワード供給ユニット及び前記クレジット管理ユニットは、前記映像信号復号化装置に取り外し可能であるように結合されているアクセスコントロール装置に含まれ、それ故、前記クレジット情報は、前記アクセスコントロール装置が前記映像信号復号化装置から取り外しされるとき、前記アクセスコントロール装置において保持されている、ことを特徴とする映像信号分配システム。
【請求項７】
請求項１に記載の映像信号分配システムであって、前記アクセスコントロール装置はスマートカードである、ことを特徴とする映像信号分配システム。
【請求項８】
映像信号再生装置であって：
暗号化映像信号と、映像信号を復号化するためのコントロールワード情報と、前記映像信号のそれぞれの一部を視聴するための料金を示す料金情報と、を有するデータストリームを受信するための受信入力；
前記受信入力及びコントロールワード出力に結合された入力を有し且つ前記コントロールワード情報からもたらされるコントロールワードを供給するように備えられているコントロールワード供給ユニット；
前記受信入力に結合されている映像入力と前記コントロールワード出力に結合されているコントロールワード入力とを有する映像信号復号化装置であって、前記コントロールワードを用いて前記映像情報を復号化するように備えられている、映像信号復号化装置；並びに
クレジットメモリを有するクレジット管理ユニットであって、前記クレジットメモリがクレジットの閾値以上の利用可能性を示すかどうかに依存して、コントロール情報を前記コントロールワードの供給をイネーブルに又はディセーブルにすることを可能にするように、そして前記コントロールワードが供給される復号化のために前記映像信号の一部についての料金情報に従って前記クレジットメモリにおけるクレジットの金額を減額するように、備えられているクレジット管理ユニット；
を有することを特徴とする映像信号再生装置。
【請求項９】
請求項８に記載の映像信号再生装置であって、前記ストリームは暗号化コントロールメッセージを有し、前記暗号化コントロールメッセージは暗号化コントロールワード及び鍵情報の両方を有し、前記コントロールワード供給ユニットは、前記映像信号再生装置における秘密情報及び前記暗号化コントロールメッセージの特定の一における鍵情報からもたらされる鍵を決定するように、そして前記もたらされた鍵を用いて前記暗号化コントロールメッセージの特定の一から前記暗号化コントロールワードを復号化するように、備えられている、ことを特徴とする映像信号再生装置。
【請求項１０】
請求項８に記載の映像信号再生装置であって、前記ストリームは、前記料金情報の一部と前記暗号化コントロールワードのそれぞれの一を有する暗号化コントロールメッセージを有し、前記コントロールワード供給ユニットは、前記暗号化コントロールメッセージの特定の一からの前記コントロールワードが映像情報を復号化するために用いられるとき、前記暗号化コントロールメッセージの特定の一おける前記料金情報の一部に従って前記クレジットの料金を減額するように備えられている、ことを特徴とする映像信号再生装置。
【請求項１１】
請求項１０に記載の映像信号再生装置であって、前記コントロールワード供給ユニットは、前記暗号化コントロールメッセージにおいて含まれる鍵情報及び前記コントロールワード供給ユニットを有するセキュア装置に局部的な秘密情報を用いてもたらされる認証情報を用いて、前記暗号化コントロールメッセージを認証するように備えられている、ことを特徴とする映像信号再生装置。

【請求項１２】
請求項８に記載の映像信号再生装置であって、前記コントロールワード供給ユニットは利用可能な秘密情報の複数のアイテムを有し、前記ストリームはアイテム選択情報を有し、前記コントロールワード供給ユニットは、前記アイテム選択情報のコントロールの下で選択される選択情報の前記アイテムの特定の一と前記鍵情報を用いて、前記鍵から前記もたらされた鍵を生成するように備えられ、前記もたらされた鍵は前記暗号化コントロールワードを復号化するように用いられる、ことを特徴とする映像信号再生装置。
【請求項１３】
請求項８に記載の映像信号再生装置であって、前記コントロールワード供給ユニット及び前記クレジット管理ユニットは、前記受信入力及び前記映像信号復号化装置に取り外し可能であるように結合されているアクセスコントロール装置に含まれている、ことを特徴とする映像信号再生装置。
【請求項１４】
請求項１３に記載の映像信号再生装置であって、前記アクセスコントロール装置はスマートカードである、ことを特徴とする映像信号再生装置。
【請求項１５】
請求項７に記載の映像信号再生装置であって、スリープタイマーを有し、前記クレジット管理ユニットは、前記スリープタイマーの期限が切れるとき、前記コントロールワードの供給をイネーブルにすること及びを前記クレジットの金額を減額することを停止するように備えられている、ことを特徴とする映像信号再生装置。
【請求項１６】
請求項１５に記載の映像信号再生装置であって、前記クレジット管理ユニットは、閾値と所定の時間期間において生じた前記クレジットの金額の減額を比較するように、そして前記コントロールワードの供給をイネーブルにし且つ前記閾値を上回るときに前記時間期間において前記クレジットの金額を減額することを停止するように、備えられている、ことを特徴とする映像信号再生装置。
【請求項１７】
請求項８に記載の映像信号再生装置であって、パスワード情報を受信するためのユーザ入力を有し、前記クレジット管理ユニットは、前記コントロールワードの供給をイネーブルにし、そして前記ユーザ入力において所定のパスワードの入力時に条件付きの前記クレジットの金額を減額するように備えられている、ことを特徴とする映像信号再生装置。
【請求項１８】
請求項８に記載の映像信号再生装置であって、前記クレジット管理ユニットは、前記コントロールワードの供給及び前記クレジットの金額の減額をイネーブルにするための条件を特定する複数のユーザ選択可能特性の選択可能な一を実行するように備えられている、ことを特徴とする映像信号再生装置。
【請求項１９】
請求項８に記載の映像信号再生装置であって、前記データストリームから前記料金情報を抽出するように備えられている受信器を有する、映像信号再生装置であり、ディスプレイ装置は、前記料金情報を用いて前記クレジット情報の減額及び前記料金情報に関連する前記映像情報の復号化をイネーブルにすることに先立って、前記受信器に結合され、そして前記抽出された料金情報を表す情報を表示するように備えられている、ことを特徴とする映像信号再生装置。
【請求項２０】
映像信号を再生する方法であって：
暗号化映像信号と、前記映像信号を復号化するためのコントロールワード情報と、前記映像信号のそれぞれ一部を視聴するための料金を表す料金情報と、を有するデータストリームを受信する段階；
前記映像情報を復号化するようにコントロールワードを用いる段階；並びに
前記コントロールワード情報から前記コントロールワードを引き出し、スマートカード

におけるクレジットメモリがクレジットの閾値の金額以上の利用可能性を示すときに前記映像情報を復号化するためにコントロールワードの導出及び／又は使用をイネーブルにするように、そしてコントロールワードが供給される復号化のための前記映像信号の前記一部についての前記料金情報に従って前記クレジットメモリにおいて前記クレジットの金額を減額するように、前記スマートカードを用いる段階；
を有することを特徴とする方法。
【請求項２１】
請求項２０に記載の方法であって、前記ストリームは暗号化コントロールメッセージを有し、前記暗号化コントロールメッセージの少なくとも一部は暗号化コントロールワード及び鍵情報の両方を有し、前記方法は、前記スマートカードにおいて、前記暗号化コントロールメッセージの特定な一における鍵情報からの導出鍵を決定する段階と、前記導出鍵を用いて前記暗号化コントロールメッセージの前記特定の一から前記暗号化コントロールワードを復号化する段階と、を有する、ことを特徴とする方法。
【請求項２２】
映像ストリームソース装置であって：
コントロールワードを用いて復号化のための映像信号を暗号化するため且つデータストリームにおいて前記暗号化された映像信号を有するための映像信号暗号化ユニット；並びに
前記データストリームにおいて暗号化コントロールメッセージを生成するための暗号化コントロールメッセージ生成器であって、前記暗号化コントロールメッセージの少なくとも一部は、暗号化コントロールワードと、前記暗号化コントロールワードを復号化するために必要な鍵情報と、前記暗号化コントロールメッセージを用いるための料金を表す料金情報と、を有する、暗号化コントロールメッセージ生成器；
を有することを特徴とする方法。
【請求項２３】
映像信号を分配する方法であって：
暗号化映像信号を有するデータストリームを生成する段階；
前記ストリームにおいて暗号化コントロールメッセージを含み、暗号化コントロールワード及び前記暗号化コントロールワードを復号化するために必要な鍵情報の両方を前記暗号化根とロースメッセージの少なくとも一部に挿入する段階；並びに
前記暗号化コントロールメッセージを用いるための料金を表す料金情報を含む段階；
を有することを特徴とする方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、映像ストリームに条件付きアクセスを与えるための映像信号分配システムと、映像ストリームに条件付きアクセスを与えるための方法及び装置と、暗号化映像ストリーム及び映像ストリーム信号を生成するための方法及び装置に関する。
【背景技術】
【０００２】
特許文献、国際公開第９８／２１８５２号パンフレットにおいて、ＭＰＥＧ－２規格に準拠した条件付きアクセスシステムについて記載されている。そのようなシステムの活用はサブスクリプションに基づくものであり、そのシステムは、加入者の復号化器にメッセージ（ＥＭＭ：暗号化管理メッセージ）を送信し、種々の映像プログラムにアクセスする

ように権利が与えられる加入者のデータベースを管理する。ＥＭＭは特定の復号化器（又は、更に正確には、復号化器におけるスマートカード）に方向付けられ、加入者が視聴する権利を与えられている映像ストリームを復号化器が復号化することを可能にする。暗号化映像データは、全ての復号化器に方向付けられ且つ復号化器が復号化する暗号化コントロールワードを有する更なるメッセージ（ＥＣＭ：暗号化コントロールメッセージ）と共に送信されるが、そのようにされることが可能である場合に、映像データが復号化されるようになされるものである。

【０００３】

そのようなサブスクリプションに基づく活用は、複雑な機構であって、加入者のデータベースを有するコンピュータが備えられる必要があり、加入者についての秘密情報を保護するための手段がとられる必要があり、ＥＮＭＭを生成し且つ選択された加入者にそれらのＥＭＭを送信するためのハードウェアが備えられる必要があり、受信料金が累算される必要がありそしてその累算された受信料金がデータベースに記録される必要がある、機構を必要とする。

【０００４】

非常に簡単化された機構は、中央の場所からの加入者向けの情報を受信する必要なく、映像ストリームにアクセスすることができる権利を復号化器自体が管理する場合に可能である。これは、プリペイド活用モデルにおいて実現されることが可能であり、スマートカード（又は、他のセキュア装置）を有する復号化器は一般の視聴クレジットを備え、その一般の視聴クレジットは、十分な視聴クレジットが存在する限り、スマートカードが何れのプログラムを復号化することを可能にし、ビューアによる選択の際にプログラムが復号化されるときにスマートカードは視聴クレジットを減額する。この場合、ビューアは、一般視聴クレジットを有するスマートカードを購入することができ、ビューアのスマートカードにおける一般視聴クレジットを更新することができる。中央登録又は権利を有するＥＭＭの送信の必要はない。

【０００５】

更に、各々のスマートカード（又は、他のセキュア装置）は、好適には、何れのプログラムを復号化するためにコントロールワードを復号化するように秘密情報を与えられることが可能である。それ故、特定のスマートカードにアドレスされた鍵を有するＥＭＭを送信する必要はなく、そのことは、条件付きアクセスを必要とする機構を非常に簡略化するものである。

【０００６】

しかしながら、何れの時点で何れのプログラムのコントロールワードを復号化するように鍵を有する複数の自由に利用可能であるスマートカード（又は、他のセキュア装置）を備える場合、及び、全てのプログラムが、それらのコントロールワードが同じ鍵を用いて復号化されることができる場合、セキュリティのリスクが入り込む。非認証アクセスを得ることを所望する人は、非常に多くの暗号化コントロールワードをそれらの復号化される相手と比較する機会を得ることが可能であり、そのことは、鍵の再生を容易にする。又、鍵に関する情報が、映像情報を復号化する演算子の機構からリークする場合、全体的なシステムが危険にさらされることとなる。

【特許文献１】国際公開第９８／２１８５２号パンフレット

【発明の開示】

【発明が解決しようとする課題】

【０００７】

特に、本発明の目的は、コストを管理する中央の加入者データベースを必要とすることなく、条件付きのアクセスを与える映像情報を供給することを可能にすることである。

【０００８】

特に、本発明の目的は、中央の加入者データベースを必要とすることなく、及び映像情報を復号化することを必要とするコントロールワード全てを復号化するように同じ鍵を用いることなく、条件付きのアクセスを与える映像情報を供給することを可能にすることで

ある。

【０００９】

特に、本発明の目的は、コストを管理する中央の加入者データベースを必要とすることなく、条件付きのアクセスを与える一方、鍵情報のリークを防止する可能性を与える、映像情報を供給することを可能にすることである。

【００１０】

特に、本発明の目的は、コストを管理する中央の加入者データベースを必要とすることなく、条件付きのアクセスを与える一方、映像情報のプログラムを視聴するためのクレジットの非常に適切な使用を可能にする、映像情報を供給することを可能にすることである。

【課題を解決するための手段】

【００１１】

本発明に従った映像再生装置は、映像情報を視聴するためのクレジットの金額に関する情報を記憶するためにクレジットメモリ有するクレジット管理ユニットを有する。そのクレジットメモリは、好適には、プリペイドカードとして購入することができる取り外し可能なスマートカード（又は、他のセキュア装置）の一部である。映像情報は、その映像情報の特定の一部を視聴することにより消費されるクレジットを表す料金情報を又、含むストリームに含まれる。再生装置は、その情報が復号化されるときにクレジットメモリにおけるクレジットの金額が減額される程度を制御するようにそのストリームからの料金情報を用い、そして、十分なクレジット（典型的には、ゼロクレジット以上）が存在するときにコントロールワードの復号化を可能にする。

【００１２】

実施例においては、データストリームは、暗号化コントロールワードを復号化するように鍵を導出することに対して全てのセキュア装置にアクセス可能である暗号化コントロールワード及び鍵情報を制御する。好適には、暗号化コントロールワード及び鍵情報の両方は暗号化コントロールメッセージに含まれ、更に好適には、暗号化コントロールメッセージにおける鍵情報は、同じメッセージにおいてコントロールワードを復号化するように機能する。好適には、ＥＭＭは全く用いられず、少なくとも、特定のスマートカードにおいてＥＭＭは導出されない。

【００１３】

鍵は、例えば、スマートカード（又は、他のセキュア装置）において記憶されている秘密鍵を用いて鍵情報に暗号化演算を適用することにより、鍵情報から導出されることが可能である。他の実施形態においては、例えば、擬似ランダムシーケンスにおいて、異なる鍵は、一連の鍵を生成ためのシードとして鍵情報を用いることにより同じ鍵情報から導出されることが可能である。

【００１４】

好適には、料金情報は又、暗号化コントロールワード及び任意の鍵情報と共に、暗号化コントロールメッセージに含まれる。好適には、特定の暗号化コントロールメッセージからの料金情報は、復号化された後にその特定の暗号化コントロールメッセージからコントロールワードが供給されるとき、クレジットの料金を減少させるように用いられる。又、好適には、暗号化コントロールメッセージは、復号化コントロールワードを供給する前に認証される。認証は、好適には、暗号化コントロールメッセージからのコントロールワードを復号化するように又、用いられる同じ鍵情報から導出される認証情報を用いて実行される。

【００１５】

再生装置は、クレジットの不所望の消費に対する保護を与える。一実施形態においては、料金情報は、クレジットの支出における復号化の前及び／又は復号化の間に、ユーザに示される。他の実施形態においては、スリープタイマーの期限切れが、クレジットの消費を停止するために用いられる（スリープタイマーは、ユーザが彼又は彼女の存在を最後に確認した後、所定の時間間隔の期限を切る）。他の実施形態においては、閾値が所定の時

間期間、例えば、１日を超えた場合に、消費を停止するように、クレジット消費の閾値が用いられる。他の実施形態においては、パスワードが、クレジット消費を可能にするように用いられる。パスワードは、クレジット消費の全部を又は閾値を超えることを可能にするために必要とされることが可能である。種々の保護特性は、過剰な消費に対する保護をどのように実現させるかをユーザが選択することを可能にするように支援することが可能である。

【００１６】

本発明の上記の及び他の実施形態については、以下、非制限的な実施例を用いて、図を参照して詳述する。

【発明を実施するための最良の形態】

【００１７】

図１は、映像分配システムを示している。そのシステムは、映像ストリームソース１０と分配媒体１４を介して結合された複数の映像再生装置１２とを有する。分配媒体１４は、象徴的に示されているが、例えば、ケーブル分配ネットワーク、無線送信媒体等である。

【００１８】

映像ストリームソース１０は、映像信号入力１００と、映像暗号化ユニット１０２と、ＥＣＭ生成器１０４と、多重化器１０５と、コントロールワードソース１０６と、シードソース１０７と、鍵生成器１０８と、コントロールワード暗号化ユニット１０９とを有する。映像暗号化ユニット１０２は映像信号入力１００に結合した映像入力を有する。多重化器１０５は、映像暗号化ユニット１０２及びＥＣＭ生成器１０４の出力に結合された多重入力と、分配媒体１４に結合された出力とを有する（簡略化のために、多重化器１０５と分配媒体１４との間に典型的に有する送信器を示していない）。コントロールワードソース１０６は、コントロールワードを供給するための出力を有し、映像暗号化ユニット１０２のコントロールワード入力とコントロールワード暗号化ユニットを介してＥＣＭ生成器１０４と結合されている。シードソース１０７は、ＥＣＭ生成器１０４及び鍵生成器１０８に結合されたシード出力を有する。鍵生成器１０８は、鍵を生成するためにシードを用いるように備えられ、コントロールワード暗号化ユニット１０９に結合された鍵出力を有する。

【００１９】

映像再生装置１２各々は、実質的に同じ構造を有する。映像再生装置１２の１つについて詳細に示している。映像再生装置１２は、受信器１２０と、映像復号化ユニット１２１と、他の映像処理ユニット１２２と、セキュア装置１２４（例えば、スマートカード）とを有する。分配媒体１４は受信器１２０の入力に結合され、映像復号化ユニット１２１及びセキュア装置１２４に結合された出力を有する。映像復号化ユニット１２１は、他の映像処理ユニット１２２に結合された映像出力を有し、例えば、復号化された映像情報を表示するための表示ユニット及びＭＰＥＧ符号器を有することが可能である。

【００２０】

セキュア装置１２４は、コントロールワード復号化ユニット１２５と、鍵生成器１２６と、鍵メモリ１２７と、クレジットメモリ１２８とを有する。コントロールワード復号化ユニット１２５は、ストリームからＥＣＭを受信するために受信器１２０に結合された入力と、映像復号化ユニット１２１のコントロールワード入力に結合されたコントロールワード出力とを有する。鍵生成器１２６は、ストリームからＥＣＭを受信するために受信器１２０に結合された入力と、鍵メモリ１２７に対するインターフェースと、コントロールワード復号化ユニット１２５に結合された鍵出力とを有する。

【００２１】

動作中、映像ストリームソース１０は映像信号を受信し、この信号を暗号化し、データストリームにおいて暗号化信号を有し、暗号化映像信号を復号化するために暗号化コントロールワードを有するＥＣＭを付加する。各々の映像再生装置１２はデータストリームを受信し、ＥＣＭから暗号化コントロールワードを抽出し、そして映像信号を復号化するよ

うにそれらの暗号化コントロールワードを用い、その映像信号は、次いで、ディスプレイのために用いられることが可能である。

【００２２】

ＥＣＭ生成器１０４はＥＣＭに料金情報を加える。料金情報は、映像信号、又は、好適には、料金情報を有するＥＣＭにおけるコントロールワードにより復号化されることができる映像信号の一部をみるために支払われなければならない料金サイズを示す。映像再生装置１２は料金情報を読み出す。ビューアが、特定の時間インターバルの間、映像信号から特定のプログラムをみることを選択するとき、映像再生装置１２は映像情報を復号化し、料金サイズに比例してクレジットメモリ１２８において表されているクレジットの金額を減らす。クレジットの金額がゼロまで減らされたとき、映像再生装置１２は映像情報の復号化をディスエーブルにする。（単一のプログラムされたプロセッサ１２５は、コントロールワード復号化ユニット及びクレジット管理ユニットの両方として機能することが可能である。それに代えて、勿論、別個のクレジット管理ユニットをコントロールワード復号化ユニットとクレジットメモリとの間で用いることが可能である。）

図１に示す実施形態のシステムにおいて、ユーザは、ストリームからのプログラムと時間インターバルと（暗示的に又は明示的に）を受信器１２０に示し、その時間インターバルの間に、プログラムは復号化される必要がある。受信器１２０は、その時間インターバルの間に、選択されたプログラムのためのＥＣＭからコントロールワード復号化ユニット１２５に暗号化コントロールワード及び料金情報を供給する。クレジットメモリ１２８は、利用可能なクレジットの金額に関する情報を記憶する。そのクレジットメモリが料金情報及び暗号化コントロールワードを受信するとき、コントロールワード復号化ユニット１２５は、十分なクレジットの金額が利用可能であるかどうかについて、クレジットメモリのコンテンツを調べる。十分なクレジットの金額が利用可能である場合、コントロールワード復号化ユニット１２５はコントロールワードを復号化し、映像復号化ユニット１２１に復号化コントロールワードを供給し、そして受信された料金情報に比例してクレジットの金額を減らす。

【００２３】

このようにして、プリペイドビューが実現することが理解できる。セキュア装置１２４は、例えば、所定金額のクレジットを表す情報をクレジットメモリ１２８が有する状態で、ユーザが小売店で物理的に購入できるスマートカードである。映像再生装置１２にそのようなスマートカード１２４を挿入することにより、ユーザは、映像ストリームにおいて含まれる料金情報及びクレジットの金額に従った映像情報の量をみる機会を得る。更に、クレジットを得る他の方法を用いることが可能であることが理解できる。例えば、小売店は、クレジットメモリのコンテンツを更新する、スマートカード１２４にクレジットを“リチャージ”するための装置を備えることが可能である。セキュア装置１２４は、例えば、クレジットカード番号を用いるインターネットによる支払いの後、インターネット接続により、同様にリチャージされることが可能である。しかしながら、これは、リチャージ装置のことが忘れられ得るため、不正行為の特定の付加的リスクを必然的に伴う。他の解決方法としては、クレジットの金額の更新が媒体１４により送信されることが可能である。この場合、特定のセキュア装置に安全にアドレスすることが可能である更新メッセージが映像ソース１０により送信される必要があり、セキュア装置１２４がクレジットを受ける必要があるか否かの決定をするための機構が必要である。

【００２４】

映像ストリームソース１０は、同時に、映像復号化装置１２全てに対してコントロールワードを復号化するための復号化鍵を供給する。復号化鍵は、シードソース１０７及び鍵生成器１０８を用いて生成される。ＥＣＭ生成器１０４は、映像暗号化装置１２に送信されるＥＣＭにおけるシードソース１０７からのシード情報を有する。鍵生成器１０８は、次のように、例えば、シード情報に対して暗号化Ｅ（）演算子を適用することにより、鍵Ｋを生成するようにシード情報“ＳＥＥＤ”を用いる。

【００２５】

Ｋ＝Ｅ（ＳＥＥＤ）

この例においては、暗号化演算子Ｅ（）はシード情報ＳＥＥＤを暗号化するように秘密ルート鍵を用いる。

【００２６】

コントロールワードソース１０６はコントロールワードを生成し、それらのコントロールワードは、映像情報を暗号化するように映像暗号化ユニット１０２により用いられる。コントロールワード暗号化ユニット１０９は、コントロールワードを暗号化するように生成され且つＥＣＭに含まれるようにＥＣＭ生成器１０４に暗号化コントロールワードを供給する。それ故、ＥＣＭは、コントロールワードを暗号化するために鍵を生成するように用いられるシードＳＥＥＤばかりでなく、暗号化コントロールワードを有する。

【００２７】

図１ａは他の実施形態を示し、その図においては、映像ストリームソースは２つの構成要素であって、信頼された第三者ユニット１０ａ及びヘッドエンド１０ｂを有する。信頼された第三者ユニット１０ａのみがルート鍵ＫＲにアクセスすることができる。信頼された第三者ユニット１０ａはシードを生成し、鍵Ｋを生成するようにルート鍵を用いる。信頼された第三者ユニット１０ａはシード及び鍵Ｋを送信する（後者は、暗号化ユニット１０００により鍵暗号化鍵ＫＥＫを用いる暗号化の後である）。ヘッドエンドにおいては、鍵Ｋは復号化ユニット１００２により復号化され、ＥＣＭに含まれるように及びコントロールワード生成器１０６により生成されたコントロールワードを暗号化するように用いられる。鍵暗号化鍵ＫＥＫは信頼された第三者ユニット１０ａにおいてソース１００４により供給され、それに対応する復号化はヘッドエンド１０ｂにおいて供給される。信頼された第三者ユニット１０ａは別個のユニットであり、ヘッドエンド１０ｂの演算子に対してアクセス可能でない。このようにして、情報がヘッドエンド１０ｂにおいて不正にアクセスされる場合、ルート鍵は危うくされない。

【００２８】

映像再生装置１２においては、鍵生成器１２６はシード情報ＳＥＥＤを受信し、コントロールワードを復号化するために鍵Ｋを生成するようにこの情報を用いる。鍵Ｋは、例えば、映像ストリームソースにおいて用いられた同じ秘密ルート鍵ＫＲを用いてシードを暗号化することにより生成されることが可能である。鍵生成器１２６は鍵メモリ１２７からこの鍵を取り出す。発行されたクレジットの管理が何らなされない、それ故、セキュア装置に特定の鍵メッセージが映像ストリームソースから送信されないとき、多くのセキュア装置は同じルート鍵を供給されなければならない。好適には、生成された鍵は、秘密ルート鍵のハッキングが更に困難になるようにセキュア装置１２４において保たれる。

【００２９】

図２は、映像産生装置における鍵の生成について示している。ＥＣＭからのシード情報は、鍵Ｋを生成するようにルート鍵ＫＲを用いる暗号演算２０において用いられ、ＥＣＭからの暗号化コントロールワード情報からコントロールワードＣＷを復号化するように複合演算２２において用いられる。同様に、ＥＣＭからのシード情報は、認証鍵Ｋを生成するように認証ルート鍵ＡＫＲを用いる暗号化演算２４において用いられることが可能であり、ＥＣＭからの情報を用いる復号化をイネーブル又はディセーブルにするように認証演算２６において用いられる。

【００３０】

好適には、ＥＣＭからのコントロールワードを復号化するために必要なシード情報ＳＥＥＤは同じＥＣＭに含まれている。それ故、映像データは、一旦、ＥＣＭが受信されると、殆ど瞬時に復号化されることが可能である。しかしながら、他の実施形態においては、シード情報はＥＣＭのサブセットのみに含まれる。この場合、鍵生成器１２６又はコントロールワード複合ユニット１２５は反復使用のために生成された鍵を記憶する。この場合、ＥＣＭからのシード情報は、シード情報を有するＥＣＭにおいてコントロールワードを適用する必要性を有することなく、後のＥＣＭにおいてコントロールワードを適用することが可能である。しかしながら、好適には、シード情報は、シード情報を用いて復号化さ

れる暗号化コントロールワードと共に実質的に同時に含まれる。ここで用いる表現“同時に”は、異なる場所からのデータが映像データの再生中に再生される時点の間の時間遅延に関するストリームにおける場所の違いを意味し、“実質的に同時に”は、たとえあるとしても、遅延は非常に小さいため、その遅延中、映像信号がないことは、全再生映像情報についての人間の理解から除外されないことを意味する。

【００３１】

シード情報は、コントロールワードが変わる各々のとき、変わることが可能である。これは、鍵のハッキングの可能性を減少させる。しかしながら、本発明から逸脱することなく、シードは、異なる時間に、例えば、コントロールワードより非常に小さい頻度で、例えば、数時間毎に、又は、コントロールワードにおける変化に対する位相オフセットを伴って、変わることが可能である。

【００３２】

他の実施形態においては、同じシード情報ＳＥＥＤが、映像ストリームソース１０及び映像再生装置１２において同期状態で複数の鍵の生成が行われるように用いられることが可能である。擬似ランダム生成関数Ｒが、例えば、映像ストリームソース１０及び映像再生装置１２の両方において連続的なシードを生成するように、シードに適用されることが可能である。ここで、ＳＥＥＤ（ｎ）＝Ｒ（ＳＥＥＤ（ｎ－１））であり、ＳＥＥＤ（）はＥＣＭから得られるシードである。このことは、送信される必要があるシード数を低減させるが、不可欠ではない。

【００３３】

好適には、セキュア装置１２４（例えば、コントロールワード復号化ユニット１２５）は、コントロールワードを供給する前に不正使用できないサインについてＥＣＭからの暗号化コントロールワードを調べる。これは、ＥＣＭのハッシュ関数を演算し且つ基準値と結果を比較することにより、又は、認証鍵ＡＫを用いてＥＣＭを暗号化し且つストリーム内に供給される基準値とこの暗号化からもたらされた結果を比較することにより実現される。実施形態のおいては、このような目的のために用いられる認証鍵ＡＫは、復号化鍵と同じシード情報ＳＥＥＤから演算されるが、ルート鍵ＫＲと異なり且つ映像ストリームソース１０及びセキュア装置１２４の両方において記憶される認証ルート鍵ＡＫＲを用いる。

【００３４】

映像ストリームソース１０を管理する機構からのリークに対する保護として、映像再生装置の各々のセキュア装置１２４における鍵メモリ１２７は、好適には、複数のルート鍵ＫＲ（例えば、４つのルート鍵）及び、任意に、複数の認証ルート鍵ＡＫＲを記憶する。鍵が危うくされたことを発見するとき、記憶されている鍵と異なる鍵が用いられることが可能である。この目的で、ＥＣＭは、コントロールワードを復号化するための鍵Ｋを生成するように用いられる必要があるルート鍵ＫＲを表す選択情報を表す選択情報を有する。鍵生成器１２６は、ＥＣＭからこのような選択情報を読み出し、従って、鍵メモリ１２７からルート鍵を選択する。ルート鍵が危うくされた後、そのルート鍵は、セキュア装置１２４において記憶されている鍵に対応する鍵により、映像ストリームソース１０の鍵生成器１０８において置き換えられ、ＥＣＭ生成器１０４は新しい鍵を選択するための選択情報を有する。

【００３５】

映像ストリームソース１０は、料金情報を受信するための入力を有する。その料金情報は、例えば、入力１００の映像ストリームにおいて含まれ、ＥＣＭに含まれるようにＥＣＭ生成器１０４に供給されることが可能である。代替として、それぞれのプログラム及び時間インターバルに対する料金についての識別を有するファイルが、含まれるように、ＥＣＭ生成器１０４に供給されることが可能である。

【００３６】

好適には、時間インターバルにおけるプログラムについての料金情報は、その時間インターバルにおいてプログラムを復号化するために必要なコントロールを有する各々のＥＣ

Ｍに含まれる。それ故、コントロールワード復号化ユニット１２５は、コントロールワードを有するＥＣＭにおいて料金情報に応じて各々のコントロールワードの復号化のときにクレジットの金額を減少させることができる。料金サイズは、典型的には、映像信号におけるコンテンツの特定のアイテム、例えば、スポーツの試合又は動画等の間、一定である。しかしながら、本発明から逸脱することなく、料金サイズを変えることにより、例えば、コンテンツのアイテムの開始部分では低い又はゼロの料金サイズを、又は、サッカーの試合のゴールで得点が得られるシーン、動画のクライマックス等のような、アイテムの選択された非常に関心がもたれる部分の間にはより高い料金サイズを示すことが可能である。

【００３７】

代替として、ＥＣＭ生成器は、適用される時間インターバル及びプログラム仕様によりＥＣＭの状態で料金サイズを補うことが可能である。この場合、コントロールワード復号化ユニットはその情報を記憶し、その時間インターバルにおいてそのプログラムに対して受信される料金サイズに従った時間インターバルにおいてプログラムが視聴されるとき、その料金サイズに従ってクレジットを減少させる（料金サイズが受信されていない場合、復号化はディセーブルである）。この場合、全てのＥＣＭが料金情報を有する必要はなく、そのことは空間を節約することができるが、不正使用のリスクを増大させ、そして、プログラムが視聴される前に存在する待ち時間を長くする可能性がある。

【００３８】

他の実施形態においては、料金情報は、プログラムから全体としての時間インターバル（例えば、動画又はスポーツの試合の持続時間）の間の料金に対して適用されることが可能である。この例においては、コントロールワード復号化ユニット１２５は、この時間インターバルに対して一度、クレジットメモリ１２８におけるクレジットの金額を減少させ、全体的な時間インターバルの間、そのプログラムに対してコントロールワードを実質的に供給することが可能である情報を記憶する。これは、その時間インターバルにおいてサンプリングされたビューイングを全体のインターバルの間のビューイングと同程度に高額にすることができる。

【００３９】

好適には、クレジットの不注意の又は不所望の消費に対して、幾つかの予防策が講じられる。一実施形態においては、クレジットメモリ１２８において表されているクレジットの金額は、ユーザからの信号がそのようなものであった後にのみ、減少される。一実施形態においては、受信器１２０は、例えば、リモートコントロールユニット（図示せず）から信号を受信するための入力により、プログラム選択ダイアログを開始するためにユーザからの指令を受信するように構成される。このダイアログにおいては、受信器はＥＣＭから料金情報を抽出し、この料金情報から導き出される情報が更なる映像処理ユニット１２２により表示されるようにされ、それ故、ユーザは、特定の時間インターバルの間、１つ又はそれ以上のプログラムを視聴するために必要なクレジットの金額を理解することができる。ユーザが、次に、時間インターバルにおいてプログラムを受け入れるための、又は、時間インターバルにおいて複数のプログラムから受け入れるプログラムを選択するための信号を送信するとき、受信器１２０は、クレジットの金額を減少させ、その時間インターバルにおいてそのプログラムのために復号化コントロールワードを供給することが可能であるようにセキュア装置１２４に信号を送信することによりダイアログを終了する。

【００４０】

代替として、受信器１２０は、ＥＣＭからの料金サイズに関する情報を抽出し、導き出された情報が更なる映像処理ユニット１２２による復号化情報と共に表示されるようにすることが可能である。このようにして、クレジットの金額の減額は、先ず、ユーザに知らせることなく開始されることが可能であるが、ユーザは、そのクレジットの減額が高額である場合、そのプログラムをオフに切り換えることが可能である。他の実施形態においては、クレジットの金額の減額は、プログラムの復号化をオンに切り換えた後にある遅延と共に開始されることが可能であり、それ故、料金に関する情報を見ながら、ユーザはクレ

ジットの減額を課せられることなく再び、オフに切り換えることができる。保護手段についての他の実施形態としては、ビューアが、所定の時間インターバル、例えば、３０分の間、そのビューアの存在を確認することができないとき、コントロールワード及びクレジット消費の復号化をオフに切り換えるスリープタイマーを備えることが可能である。スリープタイマーは、例えば、リモートコントロールユニットからの信号、映像再生装置１２におけるユーザボタンの作動等を用いて、リセットされることが可能である。

【００４１】

他の予防策としては、クレジットの閾値の金額以上が所定の時間インターバル内に、例えば、１日の経過において消費される場合、映像再生装置１２は、消費をオフに切り換えることが可能である。他の実施例としては、コントロールワード復号化ユニット１２５は、復号化コントロールワードの供給及びクレジットの金額の低額を開始する前に、パスワードを入力することが必要であることが可能である。これは、閾値と組み合わされることが可能であり、例えば、それ故、クレジットの閾値の金額以上が所定期間（例えば、１時間）内に消費され且つ正しいパスワードが入力されなかったとき、クレジットの消費は阻止される。

【００４２】

上記の手段が受信器１２０において実施されることが可能であり、それ故、受信器１２０は、クレジットを減額しないような条件が得られるとき、セキュア装置１２４へのＥＣＭの供給を阻止する。上記の手段の一部又は全部は又、例えば、コントロールワード復号化ユニット１２５において、セキュア装置１２４で実施されることが可能である。クレジットが消費できる条件を、セキュア装置１２４において予め設定することが可能である。それ故、ユーザが、例えば、スマートカードを購入するとき、そのユーザは、種々の保護機構又は閾値を与える種々のスマートカードの中から選択することができる。特に、パスワードを用いるチェックは、不正使用を回避するようにセキュア装置に適用されることが可能である。

【００４３】

ユーザによる制御下で閾値レベルを設定する又は所定の閾値を有するセキュア装置を備えることにより、不所望の使用に対抗する種々の保護のレベルを与えることができる。他の実施形態においては、複数の選択可能な保護の特徴を与えることができ、それらの特徴の各々は、クレジットが消費することが可能である条件自体の組み合わせを規定することができる。一構成においては、例えば、パスワードの入力なしでクレジットが消費されることが特定され、他の構成においては、パスワードの入力なしで一日でクレジットの閾値以下の金額が消費されたことを特定することが可能であり、他の構成においては、種々のプログラム等に対して種々の閾値を用いることが可能である。この場合、ユーザは、単に、例えば、受信器１２０おいて選択することにより特徴を示す必要がある。

【００４４】

図３は、ＥＣＭを生成する処理について示している。先ず、コスト表示３０、シード情報３１並びに第１及び第２コントロールワード３２、３３（代表的には、映像情報及び更なる映像情報を同時に復号化するため）を有するフィールドを有するオリジナルのメッセージＡが生成される。次に、認証フィールド３４がメッセージＢから加えられる。認証フィールドにおいては、一方向（ハッシュ）関数を用いてオリジナルのメッセージＡから演算される情報が挿入される。次に、半暗号化メッセージＣが構成され、認証フィールド３４、コストフィールド３０及びシードフィールドを有するメッセージＢの一般部分が暗号化される。最終的に、コントロールワードを有する特定部分が、他の鍵又は送信のためのメッセージを生成するための暗号化アルゴリズムを用いて暗号化される。このようにして、管理目的及びコントロールワードの抽出それぞれのために、一般部分及び特定部分に対して別個のアクセスを与えることができる。認証情報は両方のメッセージの部分から生成され、それ故、両方の部分の復号化はそれらのメッセージを認証する必要はない。代替として、一般部分は暗号化されないまま残されることが可能である。このような認証においては、特定部分の復号化は尚も必要である。

【００４５】

本発明について、特定の実施形態について上記のように、詳述したが、多くの代替の実施形態が可能であることが理解されることであろう。例えば、別個のユニット及びメモリをセキュア装置１２４において示しているが、例えば、クレジット減額、コントロールワード復号化及び鍵生成等の複数の機能を実行するように往路グラムされた汎用プロセッサ及び単一の不揮発性メモリを有することが可能であることが理解されるであろう。同様に、映像ストリームソース１０において示されている複数のユニットの機能は、適切にプログラムされたプロセッサ及び／又はそのプロセッサの組み合わせにより実行されることが可能である。

【図面の簡単な説明】

【００４６】

【図１】映像分配システムを示す図である。

【図１ａ】映像ソースを示す図である。

【図２】復号化情報フローを示す図である。

【図３】暗号化コントロールメッセージの生成を示す図である。

【図１】

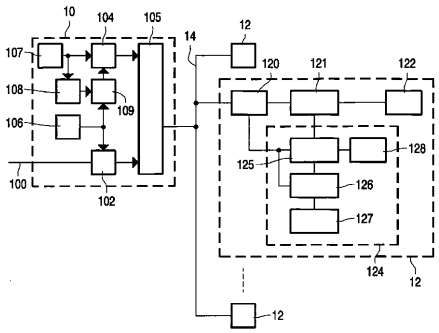


FIG. 1

【図２】

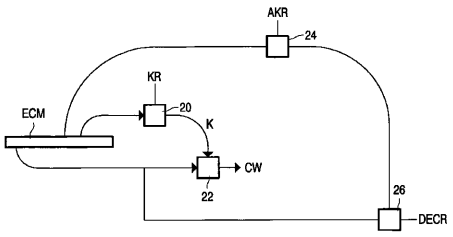


FIG. 2

【図１ａ】

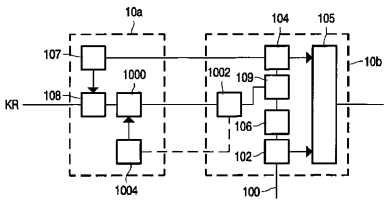


FIG. 1a

【図３】

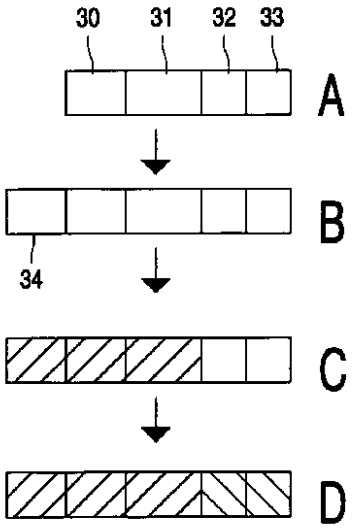


FIG. 3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/052705

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G07F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ESKICIOGLU A M ET AL: "Security of digital entertainment content from creation to consumption" SIGNAL PROCESSING. IMAGE COMMUNICATION, ELSEVIER SCIENCE PUBLISHERS, AMSTERDAM, NL, vol. 18, no. 4, April 2003 (2003-04), pages 237-262, XP004411720 ISSN: 0923-5965 pages 249-251, paragraph 5.1	1-14,17, 19-23
Y	US 6 126 069 A (STIEFEL ET AL) 3 October 2000 (2000-10-03) column 2, line 42 - column 4, line 2	1-14,17, 19-23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 February 2005	01/03/2005

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

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/052705

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 751 732 A (KAMITAKE ET AL) 14 June 1988 (1988-06-14) column 3, line 47 - column 4, line 65	1,6,8, 13,14, 19,20, 22,23
Y	WO 01/76251 A (VISA INTERNATIONAL SERVICE ASSOCIATION; CUTINO, SUZANNE, C; DAVIS, VIR) 11 October 2001 (2001-10-11)	17
A	page 7, line 27 - page 8, line 7	1,8,20, 22,23
A	GUILLOU L C ET AL: "ENCIPHERMENT AND CONDITIONAL ACCESS" SMPTE JOURNAL, SMPTE INC. SCARSDALE, N.Y, US, vol. 103, no. 6, 1 June 1994 (1994-06-01), pages 398-406, XP000457575 ISSN: 0036-1682 figures 4,5	1-23
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 paragraphs '03.2!, '03.4!, '05.1!; figures 6,7	1-23

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

ırmation on patent family members

Inte pnal Application No
PCT/IB2004/052705

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6126069	A	03-10-2000	DE	19604691 A1	14-08-1997
			EP	0789337 A2	13-08-1997
US 4751732	A	14-06-1988	JP	61020441 A	29-01-1986
			JP	61020182 A	28-01-1986
WO 0176251	A	11-10-2001	AU	4735001 A	15-10-2001
			CA	2398419 A1	11-10-2001
			EP	1264484 A2	11-12-2002
			EP	1263230 A1	04-12-2002
			WO	0176251 A2	11-10-2001

Form PCT/ISA/210 (patent family annex) (January 2004)

フロントページの続き

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

Ｆターム(参考) 5C164 FA02 PA04 PA24 SA52S SC02S SC32S TB23S TB37S UA12S UB03S UC24S
5J104 AA16 AA32 BA03 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA27 NA35 NA37 NA38 PA05 PA11