(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2008-545308
(P2008-545308A)
(43)公表日　平成20年12月11日(2008.12.11)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	7/167	(2006.01)	H04N	7/167	Z	5C164
H04L	9/36	(2006.01)	H04L	9/00	685	5J104

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

(21)出願番号　特願2008-518872 (P2008-518872)
(86)(22)出願日　平成18年7月6日 (2006.7.6)
(85)翻訳文提出日　平成20年1月30日 (2008.1.30)
(86)国際出願番号　PCT/EP2006/063989
(87)国際公開番号　WO2007/006736
(87)国際公開日　平成19年1月18日 (2007.1.18)
(31)優先権主張番号　05106186.9
(32)優先日　平成17年7月7日 (2005.7.7)
(33)優先権主張国　欧州特許庁 (EP)

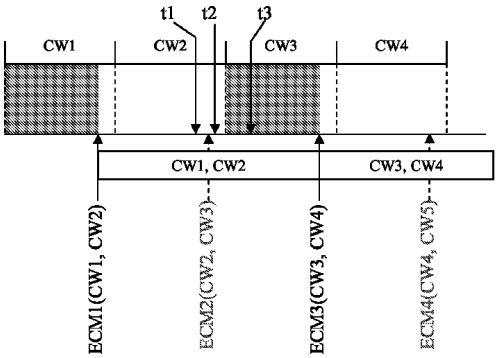
(71)出願人　504344495
ナグラビジョン　エス　アー
スイス　ＣＨ－１０３３　シュゾー－シュール－ローザンヌ，ルート　ドゥ　ジュネーヴ　２２－２４
(74)代理人　100085372
弁理士　須田　正義
(72)発明者　ストランスキ，フィリップ
スイス　ＣＨ－１０３３　シュゾー・スュール・ローザンヌ，シュマン　デ　グラン・シャン

Ｆターム(参考)　5C164 PA26 SB03S SC02P UC22S
5J104 AA12 AA16 BA03 EA08 EA17 JA03 NA37 PA05

最終頁に続く

(54)【発明の名称】暗号化されたデータへのアクセスの制御方法

(57)【要約】
本発明は、制御語（ＣＷ）により暗号化されたデータ（ＣＴ）へのアクセス制御方法に関し、これらの制御語は、制御メッセージ（ＥＣＭ）に入れられた状態でセキュリティモジュールによって受信され、暗号化データオペレーティングユニットに返送される。これらの制御メッセージ（ＥＣＭ）は少なくとも１つの第１制御語（ＣＷ１）及び第２制御語（ＣＷ２）を含み、これらの制御語によりそれぞれ、暗号有効期間（ＣＰ）と呼ばれる所定の期間、暗号化データ（ＣＴ）へのアクセスが可能である。この方法は、－　少なくとも１つのオペレーティングユニットに前記暗号化データを送信する工程と、－
制御メッセージ（ＥＣＭ）を前記オペレーティングユニットに送信する工程であって、少なくとも２つの所定の制御語（ＣＷ１、ＣＷ２）を含むそのような制御メッセージ（ＥＣＭ）が、前記第１制御語（ＣＷ１）により暗号化されたデータの送信後かつ前記第２制御語（ＣＷ２）により暗号化されたデータの送信の前にオペレーティングユニットに送信される工程とを含む。前記方法は、オペレーティングユニットへの前記第１制御語（ＣＷ



【特許請求の範囲】
【請求項１】
制御メッセージ(ECM)に入られた状態でセキュリティモジュールによって受信され、暗号化データオペレーティングユニットに返送される制御語であり、前記制御メッセージ(ECM)が少なくとも１つの第１制御語(CW1)及び第２制御語(CW2)を含み、これらの制御語によりそれぞれ、暗号有効期間(CP)と呼ばれる所定の期間、暗号化データ(CT)へのアクセスが可能である、制御語(CW)により暗号化されたデータ(CT)へのアクセス制御方法であって、
－　少なくとも１つのオペレーティングユニットに前記暗号化データを送信する工程と、
－　制御メッセージ(ECM)を前記オペレーティングユニットに送信する工程であって、少なくとも２つの所定の制御語(CW1, CW2)を含むそのような制御メッセージ(ECM)が、前記第１制御語(CW1)により暗号化されたデータの送信後かつ前記第２制御語(CW2)により暗号化されたデータの送信の前にオペレーティングユニットに送信される工程と
を含み、
オペレーティングユニットへの前記第１制御語(CW1)により暗号化されたデータの送信と、前記第１制御語(CW1)及び前記第２制御語(CW2)を含む制御メッセージ(ECM)の送信との間のずれの時間が暗号有効期間の７５％を上回ることを特徴とする方法。
【請求項２】
オペレーティングユニットへの前記第１制御語(CW1)により暗号化されたデータの送信と、前記第１制御語(CW1)及び前記第２制御語(CW2)を含む制御メッセージ(ECM)の送信との間のずれの時間が暗号有効期間の１００％未満であることを特徴とする、請求項１に記載のアクセス制御方法。
【請求項３】
オペレーティングユニットへの前記第１制御語(CW1)により暗号化されたデータの送信と、前記第１制御語(CW1)及び前記第２制御語(CW2)を含む制御メッセージ(ECM)の送信との間のずれの時間が暗号有効期間の１００％未満であり、かつそこからセキュリティモジュールによる前記制御メッセージの処理時間及びオペレーティングユニットへの制御語の返送時間を減じた時間であることを特徴とする、請求項１又は２に記載のアクセス制御方法。
【請求項４】
データストリームがＭＰＥＧタイプであることを特徴とする、請求項１に記載のアクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、制御メッセージのセキュリティモジュールによって受信され、暗号化データオペレーティングユニットに返送される制御語である、制御語ＣＷにより暗号化されたデータへのアクセス制御方法に関する。
【０００２】
本発明は有料テレビの場合に特に適用される。
【背景技術】
【０００３】
周知のように、有料テレビの上記のような分野においては、データはデータプロバイダが制御語と呼ばれる暗号化鍵を使用して暗号化される。これらのデータはユーザー又は加入者のマルチメディアユニットに送信される。これと並行して、制御語が制御メッセージストリームとしてこれらのマルチメディアユニットに送信される。
【０００４】
通常、マルチメディアユニットは、有料テレビの場合には、上記の２つのストリームを受信するデコーダとなるオペレーティングユニットと、これらのストリームの使用に関する暗号化作業を担当するセキュリティモジュールとで構成される。

【０００５】
当業者にとっては既知のように、そのようなセキュリティモジュールは本来、異なる４つの形態で作製することができる。そのうちの１つは、マイクロプロセッサカード、チップカード、より一般的は電子モジュール（キー、バッジ、...）である。通常、そのようなモジュールは取り外し可能であり、デコーダに接続することができる。電気接点を伴う形状が最も使われているが、例えばＩＳＯ１４４４３タイプの無接点結合もある。
【０００６】
既知の第２の形態は、通常、デコーダのボックス内に最終的にセットされ取り外すことができない集積回路ボックスの形態である。変形形態は、ベース又はＳＩＭモジュールコネクタなどのコネクタ上に実装された回路で構成される。
【０００７】
第３の形態では、セキュリティモジュールは、例えば、デコーダのスクランブル解除モジュール、或いはデコーダのマイクロプロセッサなど、別の機能も有する集積回路ボックス内に組み込まれる。
【０００８】
第４の実施形態では、セキュリティモジュールはハードウェアで作製されるのではなく、専らソフトウェアの形態でその機能が実行される。４つの場合においては、セキュリティーレベルは異なるが機能は同一であるので、セキュリティモジュールの作製方法又はこのモジュールが取り得る形態の如何にかかわらず、セキュリティモジュールと呼称することにする。
【０００９】
制御語を含むストリームをマルチメディアユニットが受信すると、先ず、特定のデータを復号化する権利をユーザーが持っているかどうかがチェックされる。持っている場合、制御メッセージから制御語を抽出するように、制御メッセージが復号化される。次にこれらの制御語はデータを復号化するのに使用される。
【００１０】
同じく既知のように、通常、各制御語により、送信されたデータのごく一部を復号化することができる。典型的には、１つの制御語により１０秒間の有料テレビイベントを復号化することが可能である。暗号有効期間と呼ばれるこの時間の後は、安全上の理由から、制御語が変更される。
【００１１】
許可されていない状態で、暗号化されたデータへのアクセスを得る方法として可能なものは、真正なセキュリティモジュールをともなう真正なマルチメディアユニットを使用し、全てのデコーダに制御語を配信することである。これは、サーバー又は「スプリッタ」という名称で知られている分離装置を使用することにより行うことができる。こうすることにより、ただ１つのマルチメディアユニットが、暗号化されたデータへのアクセス権の取得に関する金額を支払う一方で、複数のマルチメディアユニットからイベントにアクセスすることができる。
【００１２】
米国特許出願ＵＳ２００４／０２１５６９１（特許文献１）において記述されている発明はこの不正使用を防止しようとするものである。これを実現するには、マルチメディアユニットが制御メッセージを受信する毎に、このユニット又はそれに結合されているセキュリティモジュールが、この制御メッセージがどのチャンネルに関与しているかを判定する。チャンネルの識別子が時間情報とともに記憶される。メッセージは、それが複数の異なるチャンネルに関与しているのか同一のチャンネルに関与しているのかを判定するよう比較される。メッセージが複数の異なるチャンネルに関与している場合には、ある値だけカウンターが増分される。制御メッセージが同一のチャンネルに関与している場合には、カウンターは減分される。チャンネルが多くの回数変更されたことを示す所定のしきい値にカウンターが達すると、制御語の復号化か停止される。
【００１３】

この方法では、各制御メッセージに関するチャンネルの識別子を提供することが必要である。構成によっては、提供することができない場合がある。特に１９９２年１２月の規格ＥｕｒｏｃｒｙｐｔＥＮ５００９４号において規定されているようなメッセージを使用することにより、各チャンネルではなく、チャンネルのクラスを識別することが可能である。この場合、上で記述した発明では、ただ１つのセキュリティモジュールと１つの分離装置とを使用する複数のマルチメディアユニットの使用を阻止することはできない。

【００１４】

ＷＯ０１／１５４４８号（特許文献２）で公開された国際出願は、有料テレビシステム、より詳細には、オンデマンドビデオシステムについて記述している。このシステムにおいては、データは制御語により暗号化される。これらの制御語は、ユーザーがコンテンツにアクセスしようと所望する場合にユーザーが制御語を取得しなければならない所定の時間中のみ、ユーザーに送信される。この方法により、不正ユーザーが不法に制御語を受信してコンテンツにアクセスするというリスクは制限される。

【００１５】

しかしながらこの方法は、ユーザーがチャンネルを変えることができる従来の有料テレビシステムには適用することができない。事実、チャンネルを変える場合、このユーザーは、コンテンツにアクセスできるようになる前に、新しいチャンネルに対応する制御メッセージを受信することを余儀なくされる。

【００１６】

文献ＷＯ２００４／０７１０９１号（特許文献３）は、「早送り」又は「早戻し」モードで許可されている送り速度を最大化することを目的とする発明について記述している。この目的は本出願の対象となる目的とは全く異なる。この文献ＷＯ２００４／０７１０９１（特許文献３）では、データストリームに対し制御語の変更を暗号有効期間のほぼ半分に相当する値だけずらすことにより、送り速度の最適化が得られる。暗号有効期間の半分というこの値により、前進方向への送り速度も後退方向への送り速度も最適化することができるので、本発明の目的の達成を可能にする最適な値となる。この値から遠ざかれば遠ざかるほど、制御語をもつデータストリームをずらす優位性は低くなる。

【００１７】

周知のように、制御メッセージは、例えば５０ｍｓ毎というようなきわめて短い間隔で反復される。これは、チャンネルを変える（ザッピング）際、コンテンツへのアクセスに必要な制御語が素早く入手できることを目的とするものである。マルチメディアユニットは、制御メッセージを受信すると、同一の制御メッセージがセキュリティモジュールに１回しか送信されないように、同一の制御メッセージを選別する。以下の説明においては、同一のメッセージが使われることはないので、制御メッセージＥＣＭについて言及する時には、異なるメッセージが対象となっているものとする。

【００１８】

制御メッセージが複数の制御語を含む場合には問題が生じる。実際のところ、制御メッセージ１つにつき２つの制御語を送信するのが普通である。これには、制御語のうちの一方が使われている時、他方が復号化され記憶されるという利点がある。このような実施方法により、より確実な復号化アルゴリズムを実現することが可能になるが、従って復号化時間も長くなる。

【００１９】

そのような場合、不正なユーザーにとっては、２つの制御メッセージのうちの１つのみを使用し、使用しない方のメッセージを他のデコーダ、即ちオペレーティングユニットに送信するということが可能である。各デコーダはこのようにして自身に必要な制御語の全てを受信する。このように、原則として一人の加入者しか暗号化コンテンツへのアクセス権を持たないのに、複数のオペレーティングユニットがこのコンテンツにアクセスできる。

【００２０】

チャンネル識別子を使用しないで、ただ１つのデコーダが全ての制御メッセージを正規

に使用する場合と、異なる２つのデコーダが２つの制御メッセージのうちの一方を不正に使用する場合とを区別することができないため、この種の不正は検出がきわめて困難である。

【特許文献１】米国特許出願ＵＳ２００４／０２１５６９１
【特許文献２】ＷＯ０１／１５４４８号
【特許文献３】ＷＯ２００４／０７１０９１号

【発明の開示】
【発明が解決しようとする課題】
【００２１】
本発明は、この問題を解決し、よって、ただ１つのセキュリティモジュールによる２つのデコーダの不正使用時の暗号化コンテンツへのアクセスを防止することを目的とする。
【００２２】
また本発明の解決方法により、２つの制御メッセージのうちの一方しか使用せず他方の制御メッセージが他のデコーダに送信されるような不正なユーザーによる、暗号化コンテンツへのアクセスを少なくとも部分的に防ぐことができる。
【課題を解決するための手段】
【００２３】
本発明の目的は、制御メッセージに入れられた状態でセキュリティモジュールによって受信され、暗号化データオペレーティングユニットに返送される制御語であり、前記制御メッセージが少なくとも１つの第１制御語及び第２制御語を含み、これらの制御語によりそれぞれ、暗号有効期間と呼ばれる所定の期間、暗号化データへのアクセスが可能である、制御語により暗号化されたデータへのアクセス制御方法であって、
－　少なくとも１つのオペレーティングユニットに前記暗号化データを送信する工程と、
－　制御メッセージ（ＥＣＭ）を前記オペレーティングユニットに送信する工程であって、少なくとも２つの所定の制御語（ＣＷ１，ＣＷ２）を含むそのような制御メッセージ（ＥＣＭ）が、前記第１制御語（ＣＷ１）により暗号化されたデータの送信後かつ前記第２制御語（ＣＷ２）により暗号化されたデータの送信の前にオペレーティングユニットに送信される工程と
を含み、
オペレーティングユニットへの前記第１制御語（ＣＷ１）により暗号化されたデータの送信と、前記第１制御語（ＣＷ１）及び前記第２制御語（ＣＷ２）を含む制御メッセージ（ＥＣＭ）の送信との間のずれの時間が暗号有効期間の７５％を上回ることを特徴とする方法により達成される。
【００２４】
一般的に本発明による方法は２つの制御語を含む制御メッセージを使用する。しかしながら、２つの制御メッセージのうちの一方しか使用しないユーザーは、暗号化コンテンツの全てにアクセスできるわけではない。１つの分離装置及び同じセキュリティモジュールを共有している２人のユーザーはそれぞれ音声／映像コンテンツの一部にしかアクセスできなくなる。
【００２５】
本発明並びにその特長は、添付の図面、並びに非限定的例として示した特定の実施形態についての詳細な説明を参照することにより、より良く理解されよう。
【発明を実施するための最良の形態】
【００２６】
図１は先行技術による、時間の経過にともなう、音声／映像コンテンツストリームＣＴ、並びに制御語ＣＷを含む制御メッセージストリームＥＣＭの略図である。この図において、音声／映像コンテンツは符号ＣＷ１，ＣＷ２，．．．を付した制御語により暗号化され、これらの制御語は、限定された暗号有効期間と呼ばれる「継続時間」をもつ、即ち、この暗号有効期間に相当する期間だけ、各制御語により暗号化されたコンテンツにアクセスすることができる。図示例では、第１制御メッセージＥＣＭ１は２つの制御語ＣＷ１及

びＣＷ２を含む。この第１メッセージの配信と同時に、第１制御語ＣＷ１によりコンテンツＣＴが暗号化される。第１制御メッセージＥＣＭ１が復号化され、制御語ＣＷ１がセキュリティモジュールからデコーダに返送されると、コンテンツを復号化し使用することができる。この間に第２制御語ＣＷ２が記憶される。第２制御語は、必要時、即ち復号化すべきデータが、この制御語ＣＷ２によって暗号化されたデータである場合には使用することができる。

【００２７】

図２は図１に示す方法の不正な使用法を示す。この使用においては、第１ユーザーが第１制御メッセージＥＣＭ１を受信し、そこから制御語ＣＷ１及びＣＷ２を抽出する。第２制御メッセージＥＣＭ２は、使用されないようにするためにろ波される。制御語ＣＷ２は第１制御メッセージＥＣＭ１に入られた状態で送信されているので、制御語によりコンテンツを復号化しなければならない時に制御語ＣＷ２を使用することができる。

【００２８】

制御メッセージＥＣＭ２は第２デコーダに送信するのに使用することができる。不正な使用を検出するために、毎回の暗号有効期間の際、復号化された制御メッセージＥＣＭの数のカウントダウンを実行することが可能である。これにより、毎回の暗号有効期間の際にあまりにも多数の制御メッセージが復号化された時に行動を起こすことが可能である。しかしながら本発明の場合、暗号有効期間毎の制御メッセージ数についてのテストでは不正な使用を割り出し防止することができない、というのは、この数は、通常の使用時にただ１つのセキュリティモジュールによって復号化されるメッセージ数そのものだからである。

【００２９】

図３は本発明による方法の概略図である。この方法では、暗号化データストリームＣＴは制御メッセージストリームＥＣＭからずれている。以下の説明は、ただ１つのセキュリティモジュールによるただ１つのマルチメディアユニットの通常の使用に関するものである。

【００３０】

図３でｔ１で示すタイミングでユーザーがマルチメディアユニットを起動するか特定のチャンネルに到達する場合を例としてみることにする。この時点では、コンテンツＣＴは制御語ＣＷ２により復号化されなければならない。同じくこの時点で、第１制御メッセージＥＣＭ１が配信される。この制御メッセージＥＣＭ１は制御語ＣＷ１及びＣＷ２を含む。従ってコンテンツは制御語ＣＷ２により復号化することができる。

【００３１】

ユーザーは、ｔ２で示すタイミングでマルチメディアユニットを起動するか特定のチャンネルに到達する場合も、コンテンツを復号化するのに制御語ＣＷ２が必要になる。このタイミングでは、第２制御メッセージＥＣＭ２が配信される。第２制御メッセージは制御語ＣＷ２及びＣＷ３を含む。従ってコンテンツＣＴは制御語ＣＷ２により復号化することができる。

【００３２】

ｔ３で示すタイミングでユーザーがマルチメディアユニットを起動するか特定のチャンネルに到達する場合、方法の進行は、開始タイミングがｔ１である場合について説明した進行と同様となる。コンテンツにアクセスする場合には、制御メッセージＥＣＭ２からの制御語ＣＷ２を使用することができる。

【００３３】

従って、従来の使用方法では、ユーザーは、マルチメディアユニットを起動、又はチャンネルを変更するタイミングの如何にかかわらず、暗号化されたコンテンツにアクセスすることができることがわかる。

【００３４】

図４は本発明による方法を用いた２つのマルチメディアユニットの不正な使用方法を示す図である。この使用方法によれば、各デコーダは２つある制御メッセージのうちの１つ

しか使用しない。制御語ＣＷ１及びＣＷ２を含む第１制御メッセージＥＣＭ１をデコーダのうちの１つが使用する場合を想像することにする。タイミングｔ１でユーザーがマルチメディアユニットを起動するか当該チャンネルに到達すると、図３に図示する列の場合と全く同じことが起きる、つまり、コンテンツの復号化に必要な制御語ＣＷ２は制御メッセージＥＣＭに既に組み込まれているので、この制御語は使用可能になる。従ってコンテンツにアクセスすることができる。

【００３５】

タイミングｔ２でユーザーがマルチメディアユニットを起動するか当該チャンネルに到達する場合、コンテンツＣＴにアクセスできるようにするには、制御語ＣＷ２が必要になる。これは第１制御メッセージＥＣＭ１に入れて送信されてあるので使用可能であり、コンテンツを復号化することができる。

【００３６】

タイミングｔ３でユーザーがマルチメディアユニットを起動する場合、コンテンツにアクセスするには、制御語ＣＷ３が必要になる。この制御語は第２制御メッセージＥＣＭ２の入れて１回、第３制御メッセージＥＣＭ３に入れて１回、それぞれ送信される。上で説明したような不正な使用の場合、第２制御メッセージＥＣＭ２はこのデコーダによって使用されずに、別のデコーダに送信されてしまっている。従ってそのデコーダが含む制御語は当該レコーダーには使用できない。データストリームと制御メッセージストリームとの間にはずれがあるため、タイミングｔ３では第３制御メッセージＥＣＭ３は使用不可能である。その結果、第３制御語ＣＷ３が必要なタイミングと第３制御メッセージＥＣＭ３の送信との間の期間中はずっとコンテンツは復号化できなくなる。

【００３７】

実際には、誠実なユーザーが全てのコンテンツにアクセスできるように、データストリームＣＴと制御メッセージストリームＥＣＭとの間のずれは暗号有効期間より短くなければならない。不正ユーザーに対して最大限の罰則を課するためには、ずれはできる限り大きなものでなければならない。通常、暗号有効期間よりも若干短いずれを採用するものとする。好ましくは、このずれに、セキュリティモジュールによる前記制御メッセージの処理及び利用装置への制御語の返送の時間を加えたものが、暗号有効期間より短くなるようなずれを採用するものとする。

【００３８】

例えば、ストリーム間のずれを４秒として、５秒の暗号有効期間を設定ッすることが可能である。その結果、２つのデコーダに送信するのにただ１つのセキュリティモジュールしか使用しない場合、各デコーダは、無視できない期間、暗号化されたコンテンツにアクセスできなくなる。

【図面の簡単な説明】

【００３９】

【図１】データストリーム及び制御メッセージストリームが従来の方法で用いられる、先行技術による実施形態を示す図である。

【図２】データストリーム及び制御メッセージストリームが不正に用いられる、図１の実施形態を示す図である。

【図３】データストリーム及び制御メッセージストリームが従来の方法で用いられる、本発明による実施形態を示す図である。

【図４】データストリーム及び制御メッセージストリームが不正に用いられる、図３の実施形態を示す図である。

【図１】

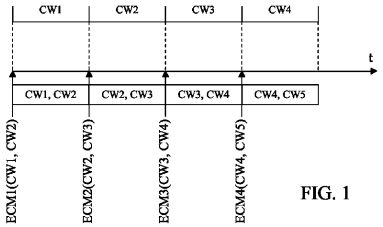


FIG. 1

【図２】

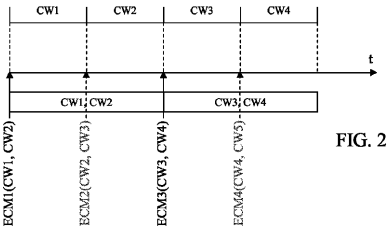


FIG. 2

【図３】

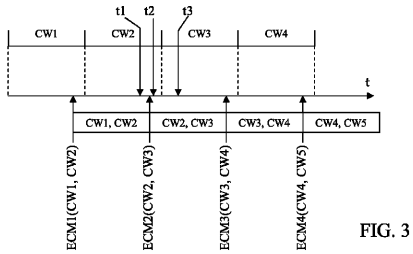


FIG. 3

【図４】

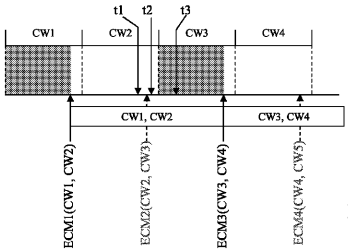


FIG. 4

【誤訳訂正書】
【提出日】平成20年2月14日(2008.2.14)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】請求項１
【訂正方法】変更
【訂正の内容】
【請求項１】
制御メッセージ(ECM)に入れられた状態でセキュリティモジュールによって受信され、暗号化データオペレーティングユニットに返送される制御語であり、前記制御メッセージ(ECM)が少なくとも１つの第１制御語(CW1)及び第２制御語(CW2)を含み、これらの制御語によりそれぞれ、暗号有効期間(CP)と呼ばれる所定の期間、暗号化データ(CT)へのアクセスが可能である、制御語(CW)により暗号化されたデータ(CT)へのアクセス制御方法であって、
－　少なくとも１つのオペレーティングユニットに前記暗号化データを送信する工程と、
－　制御メッセージ(ECM)を前記オペレーティングユニットに送信する工程であって、少なくとも２つの所定の制御語(CW1, CW2)を含むそのような制御メッセージ(ECM)が、前記第１制御語(CW1)により暗号化されたデータの送信後かつ前記第２制御語(CW2)により暗号化されたデータの送信の前にオペレーティングユニットに送信される工程と
を含み、
オペレーティングユニットへの前記第１制御語(CW1)により暗号化されたデータの送信と、前記第１制御語(CW1)及び前記第２制御語(CW2)を含む制御メッセージ(ECM)の送信との間のずれの時間が暗号有効期間の７５％を上回ることを特徴とする方法。
【誤訳訂正２】
【訂正対象書類名】明細書

【訂正対象項目名】００２７
【訂正方法】変更
【訂正の内容】
【００２７】
図２は図１に示す方法の不正な使用法を示す。この使用においては、第１ユーザーが第１制御メッセージＥＣＭ１を受信し、そこから制御語ＣＷ１及びＣＷ２を抽出する。第２制御メッセージＥＣＭ２は、使用されないようにするためにろ波される。制御語ＣＷ２は第１制御メッセージＥＣＭ１に入れられた状態で送信されているので、制御語によりコンテンツを復号化しなければならない時に制御語ＣＷ２を使用することができる。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/063989

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/167 G11B20/00

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)
H04N G11B

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, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/071091 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; ZWART, SJOERD; GERBRANDTS, PIETER) 19 August 2004 (2004-08-19) page 2, line 23 - line 25	1-4
A	WO 01/15448 A (GENERAL INSTRUMENT CORPORATION) 1 March 2001 (2001-03-01) page 7 - page 8	1-4
A	US 5 349 641 A (COUTROT ET AL) 20 September 1994 (1994-09-20) the whole document	1-4
A	EP 1 447 983 A (THOMSON LICENSING S.A) 18 August 2004 (2004-08-18) the whole document	1-4

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family 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
23 August 2006	30/08/2006

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	Bertrand, F

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/063989

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 631 193 A (LABORATOIRE EUROP RECHERC ELECTR) 10 November 1989 (1989-11-10) the whole document	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/063989

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 2004071091	A	19-08-2004	CN	1748423 A	15-03-2006
WO 0115448	A	01-03-2001	AU	7068200 A	19-03-2001
			BR	0013522 A	07-05-2002
			CA	2382701 A1	01-03-2001
			CN	1378744 A	06-11-2002
			DE	60020245 D1	23-06-2005
			DE	60020245 T2	26-01-2006
			EP	1206877 A1	22-05-2002
			JP	2003507974 T	25-02-2003
US 5349641	A	20-09-1994	CA	2103935 A1	14-02-1994
			DE	69316478 D1	26-02-1998
			DE	69316478 T2	23-07-1998
			EP	0583202 A1	16-02-1994
			FR	2694860 A1	18-02-1994
EP 1447983	A	18-08-2004	CN	1522063 A	18-08-2004
			JP	2004247036 A	02-09-2004
			US	2005105886 A1	19-05-2005
FR 2631193	A	10-11-1989	EP	0426923 A1	15-05-1991
			WO	9107849 A1	30-05-1991
			US	5224161 A	29-06-1993

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/063989

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04N7/167 G11B20/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04N G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2004/071091 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; ZWART, SJOERD; GERBRANDTS, PIETER) 19 août 2004 (2004-08-19) page 2, ligne 23 - ligne 25	1-4
A	WO 01/15448 A (GENERAL INSTRUMENT CORPORATION) 1 mars 2001 (2001-03-01) page 7 - page 8	1-4
A	US 5 349 641 A (COUTROT ET AL) 20 septembre 1994 (1994-09-20) le document en entier	1-4
A	EP 1 447 983 A (THOMSON LICENSING S.A) 18 août 2004 (2004-08-18) le document en entier	1-4

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
23 août 2006	30/08/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertrand, F

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/063989

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 631 193 A (LABORATOIRE EUROP RECHERC ELECTR) 10 novembre 1989 (1989-11-10) le document en entier	1-4

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n° PCT/EP2006/063989

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 2004071091	A	19-08-2004	CN	1748423 A	15-03-2006
WO 0115448	A	01-03-2001	AU	7068200 A	19-03-2001
			BR	0013522 A	07-05-2002
			CA	2382701 A1	01-03-2001
			CN	1378744 A	06-11-2002
			DE	60020245 D1	23-06-2005
			DE	60020245 T2	26-01-2006
			EP	1206877 A1	22-05-2002
			JP	2003507974 T	25-02-2003
US 5349641	A	20-09-1994	CA	2103935 A1	14-02-1994
			DE	69316478 D1	26-02-1998
			DE	69316478 T2	23-07-1998
			EP	0583202 A1	16-02-1994
			FR	2694860 A1	18-02-1994
EP 1447983	A	18-08-2004	CN	1522063 A	18-08-2004
			JP	2004247036 A	02-09-2004
			US	2005105886 A1	19-05-2005
FR 2631193	A	10-11-1989	EP	0426923 A1	15-05-1991
			WO	9107849 A1	30-05-1991
			US	5224161 A	29-06-1993

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,LV,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,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

【要約の続き】
１）により暗号化されたデータの送信と、前記第１制御語（ＣＷ１）及び前記第２制御語（ＣＷ２）を含む制御メッセージ（ＥＣＭ）の送信との間のずれの時間が暗号有効期間の７５％を上回ることを特徴とする。
【選択図】 図４