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

特許第5161372号
(P5161372)

(45)発行日　平成25年3月13日(2013.3.13)　(24)登録日　平成24年12月21日(2012.12.21)

(51)Int.Cl.		F I		
H04N 7/173	(2011.01)	H04N	7/173	610Z
H04H 60/16	(2008.01)	H04H	60/16	
H04H 60/23	(2008.01)	H04H	60/23	

請求項の数 5　(全 9 頁)

(21)出願番号	特願2011-527308 (P2011-527308)
(86)(22)出願日	平成21年9月16日 (2009.9.16)
(65)公表番号	特表2012-503389 (P2012-503389A)
(43)公表日	平成24年2月2日 (2012.2.2)
(86)国際出願番号	PCT/EP2009/061986
(87)国際公開番号	WO2010/031781
(87)国際公開日	平成22年3月25日 (2010.3.25)
審査請求日	平成24年7月20日 (2012.7.20)
(31)優先権主張番号	08164674.7
(32)優先日	平成20年9月19日 (2008.9.19)
(33)優先権主張国	欧州特許庁 (EP)
(31)優先権主張番号	61/136,623
(32)優先日	平成20年9月19日 (2008.9.19)
(33)優先権主張国	米国 (US)

早期審査対象出願

(73)特許権者　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　ジュノ，パスカル
スイス　ＣＨ－１３０２　ヴュフラン－ラ－ビル，ムウラン　ド　ラ　パラ　８
(72)発明者　カルロフ，アレクサンドル
スイス　ＣＨ－１２１７　メイラン，プロムナード　デ　シャン－フレッシェ　２

審査官　後藤　嘉宏

最終頁に続く

(54)【発明の名称】管理センターによって放送番組に対して受信規則を施行する方法

(57)【特許請求の範囲】

【請求項１】

受信器により受信される放送番組に対する受信規則を管理センターが施行する方法において、前記番組の受信は番組キーにより解除され、前記管理センターは複数のサブスクリプションパッケージを管理し、それに関して少なくとも１つのサブスクリプションパッケージは前記番組の受信を可能にする方法であって、

サブスクリプションパッケージごとに少なくとも肯定キーマテリアルを規定する段階であって、前記肯定キーマテリアルは少なくとも肯定キーを有し、前記サブスクリプションパッケージに契約された受信機用である、段階と、

少なくとも１つのサブスクリプションパッケージを受信した受信器のために、前記サブスクリプションパッケージの肯定キーマテリアルをロードする段階と、を含む方法であって、更に、

サブスクリプションパッケージごとに少なくとも否定キーマテリアルを規定する段階であって、前記否定キーマテリアルは少なくとも否定キーを有し、前記サブスクリプションパッケージに契約されていない受信機用である、段階と

前記受信機のために、契約がなかった前記サブスクリプションパッケージの否定キーマテリアルをロードする段階と、

前記番組が少なくとも第１サブスクリプションパッケージによって受信可能であり、少なくとも第２サブスクリプションパッケージに関して受信できない場合に、前記番組の受信を許すための許可メッセージを作成する段階であって、前記番組キー又は前記番組キー

を検索することを可能にするデータは暗号を生成するために使用され、前記第１サブスクリプションパッケージの前記肯定キーマテリアル及び前記第２サブスクリプションパッケージの前記否定キーマテリアルが前記受信器に存在する場合にのみ、前記番組キーを検索することを可能にする前記暗号が受信可能であるように、前記暗号は前記第１サブスクリプションパッケージの肯定キー及び前記第２サブスクリプションパッケージの前記否定キーの両方によって暗号化される段階と、の初期の段階
を含む方法。
【請求項２】
前記暗号が前記番組キーである請求項１記載の方法。
【請求項３】
前記暗号がセッションキーであり、前記番組キーが前記セッションキーによって暗号化され、該方法が前記暗号化された番組キーを前記許可メッセージに追加する段階を含む請求項１記載の方法。
【請求項４】
前記暗号が、少なくとも１つの否定キー及び少なくとも１つの肯定キーによって暗号を順次暗号化することにより生成される請求項１ないし３のいずれか１項に記載の方法。
【請求項５】
前記許可メッセージが前記暗号化の用に供するサブスクリプションパッケージを記載している識別情報を含む請求項１ないし４のいずれか１項に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、放送暗号化の分野、詳細には管理センター及び複数の受信装置を有する放送システムの許可権を管理する方法に関連する。
【背景技術】
【０００２】
公知の標準有料テレビ放送モデルにおいて、「限定受信方式のＥＢＵ機能論的モデル（ＥＢＵ Ｆｕｎｃｔｉｏｎａｌ Ｍｏｄｅｌ ｏｆ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ）」（ＥＢＵテクニカルレビュー、１９９５年冬）に開示されているように、放送される有料テレビ番組は暗号化され、受信側で有料テレビ番組を復号するキーは、スクランブルがかけられている有料テレビ番組と共に送られるエンタイトルメント・コントロール・メッセージ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅｓ）（ＥＣＭ）に設定される。ＥＣＭは伝達キーで暗号化され、それは、セキュリティの理由により、頻繁に変更される。
【０００３】
スクランブルを解除するキーに加えて、ＥＣＭは、受信側で施行される受信条件の形で、有料テレビ番組限定受信権に関する情報を持っている。
【０００４】
伝達キーばかりでなく個々の加入者限定受信権（例えば、１ヵ月間のサービス会員権）は、エンタイトルメント・マネージメント・メッセージ（ＥＭＭ）の形で、非同期方法で管理されて送信される。ＥＭＭは受信器にだけ知られている秘密キーによって暗号化される。
【０００５】
受信装置が番組を受信して復号することが可能であるために、第１段階は、従って、ＥＣＭメッセージを復号するのに必要な伝達キーを担送しているＥＭＭメッセージだけでなく、番組に対応する権利を担送しているＥＭＭメッセージを受信して復号することである。そのため、受信装置は固有キーを備え、ＥＭＭは受信装置の適合する固有キーによって暗号化され、この特定の装置だけがＥＭＭを復号できるように放送される。そのため、対称又は非対称のキーを使用できる。
【０００６】

いろいろな権利が受信装置のセキュリティ手段（このセキュリティ手段は通常スマートカードの形である）メモリにロードでき、次に前記セキュリティ手段により施行される。

【０００７】

これらのセキュリティ手段は、いろいろな形、例えば、スマートカード、セキュアチップ、ＵＳＢドングル、又は装置の改ざん防止ソフトウェアを有していてもよい。

【０００８】

我々は、これらのセキュリティ手段が、少なくとも伝達キーを格納するのに十分安全であると考える。固有キーは、この受信装置及びこの受信装置と関連した権利（又は複数の権利）に関係する。

【０００９】

セキュリティ手段の役割は、ＥＣＭ及びＥＭＭメッセージを受信し、伝達キーを用いてＥＣＭを復号し、受信キー（又は複数の受信キー）及びこの有料テレビ番組に関連した受信条件を抽出することである。セキュリティ手段は、ＥＣＭに含まれる受信条件に適合する権利がセキュリティ手段メモリに存在するかどうか調べ、存在する場合には、受信キーは番組を復号するために受信装置に戻される。

【００１０】

ＥＣＭは１つ以上の受信条件定義を含むことができる。この場合には、適用されるポリシーによって、セキュリティ手段はそのメモリにおける権利の存在を点検し、権利のうちの少なくとも１つが存在する場合には、受信キーを戻すことができる（ブールＯＲ機能）。別のポリシーによって、受信条件の全セットに適合するすべての権利がセキュリティ手段メモリに存在する場合にのみ、セキュリティ手段は受信キーを戻すことができる（ブールＡＮＤ機能）。

【００１１】

メモリコンテンツに関する複雑な問合わせは、特許文献１に開示されるように実行できる。さまざまな試験が肯定的な結果を与える場合にのみ、受信キーは受信装置に戻される。権利自体が考慮されるだけでなく、失効日又は信用状況も資格有効性決定においても使用できる。

【００１２】

伝達キーと同様に権利も、さまざまな方法によってセキュリティ手段メモリにＥＭＭメッセージを通してロードできる。即ち

-受信装置の初期化段階で、ホスト装置との局所接続を経由して、又は放送チャネルで送られる初期化メッセージの受信を経由して、

-いつでも、例えば、加入者のデータが変更されるときの、サービスの契約又はキャンセル、権利の更新、サービスキー（伝達キーを含む）の変更。

【００１３】

ソフトウェアのみによってなされるセキュリティ手段のアドバートによると、このソフトウェアが危険にさらされるリスクは、特定のハードウェア・セキュリティ手段の場合より高い。

【００１４】

非特許文献１において開示されているような放送暗号化プリミティブは、チャネル帯域幅、受信器の記憶容量、及び暗号化／復号の複雑さに関して放送チャネルを介してデジタルコンテンツを確実に送信する有効な方法である。それは３つのアルゴリズムから成る。セットアップ・アルゴリズム、それはシステム・パラメータ、例えば、受信器（目標）のための復号キーマテリアル及び放送センターのための暗号化キーを初期化する。暗号化アルゴリズムは認可された受信器のサブセットのための暗号を生成し、それにより認可されたサブセット以外の他の受信器は暗号を復号することができない。受信器が復号キーを備えていて、認可されたサブセットの中にある場合には、復号アルゴリズムは暗号文を正しく復号する。

【先行技術文献】

【特許文献】

【００１５】
【特許文献１】国際公開第２００４０５２００５号パンフレット
【特許文献２】欧州特許第１２５２７６８号明細書
【非特許文献】
【００１６】
【非特許文献１】Ｄａｎ　Ｂｏｎｅｈ、Ｃｒａｉｇ　Ｇｅｎｔｒｙ、及びＢｒｅｎｔ　Ｗａｔｅｒｓによる「短い暗号文及びプライベートキーによる共謀抵抗性放送暗号化（Collusion Resistant Broadcast Encryption）」
【発明の概要】
【発明が解決しようとする課題】
【００１７】
センターが、特定の基準又は特徴を満たす（又はその欠如）認可された受信器のセットに高級なコンテンツを放送することを望む状況を考慮する。この特徴は、例えば、サービスのパッケージに対する契約、スマートカードに残っている金額、受信器の郵便番号（又は他の地理的情報）、チップセット特性、あるいはその他の顧客又は装置関連の情報である可能性がある。
【００１８】
本発明の利点は、放送暗号化のプリミティブの２つの例を並行して用いることによりこの問題に効果的に対処することである。
【００１９】
比較の機能を有する特許文献１において開示された方法と異なり、本発明は放送センター（即ちヘッドエンド）で権利の施行を実行することを可能にする。前者の場合のセキュリティがセキュリティモジュールを解析して模倣する（分解する）ための問題点に基づき、その一方で、我々の場合は、セキュリティが難しい数学の問題に基づいているので、これはセキュリティモジュール（ＳＣ）において権利を施行する以前の方法より有利である。また、特許文献１の開示と異なり、本発明はシステムのセキュリティに対するいかなる影響も無しに複雑な受信条件及びポリシーを扱うことができる。
【課題を解決するための手段】
【００２０】
本発明の目的は、一方ではキーメッセージにおいて規定される受信条件を施行して、他方ではこの種の装置の受信装置又はユーザの特徴及び特性に基づいて複雑な受信条件を処理するために、受信器のセキュリティモジュール（ＳＣ）のセキュリティ手段に、より少ない程度に依存するための方法を提案することである。
【００２１】
従って、受信器により受信される放送番組に対する受信規則を管理センターが施行する方法が提案される。前記番組の受信は番組キーにより解除され、前記管理センターは複数のサブスクリプションパッケージを管理し、それに関して少なくとも１つのサブスクリプションパッケージは番組の受信を可能にする。方法は以下の初期段階を含む。
- サブスクリプションパッケージごとに少なくとも肯定キーマテリアルを規定する段階であって、前記肯定キーマテリアルは少なくとも肯定キーを有し、前記サブスクリプションパッケージに契約された受信機用である、段階と、
- 少なくとも１つのサブスクリプションパッケージを受信した受信器のために、前記サブスクリプションパッケージの肯定キーマテリアルをロードする段階とを含み、更に
サブスクリプションパッケージごとに少なくとも否定キーマテリアルを規定する段階であって、前記否定キーマテリアルは少なくとも否定キーを有し、前記サブスクリプションパッケージに契約されていない受信機用である、段階と
前記受信機のために、契約がなかった前記サブスクリプションパッケージの否定キーマテリアルをロードする段階と、
前記番組が少なくとも第１サブスクリプションパッケージによって受信可能であり、少なくとも第２サブスクリプションパッケージに関して受信できない場合に、

- 番組の受信を許すための許可メッセージを作成する段階であって、番組キー又は番組キーを検索することを可能にするデータは暗号を生成するために使用され、第１サブスクリプションパッケージの肯定キーマテリアル及び第２サブスクリプションパッケージの否定キーマテリアルが受信器に存在する場合にのみ、番組キーを検索することを可能にする暗号が受信可能であるように、前記暗号は第１サブスクリプションパッケージの肯定キー及び第２サブスクリプションパッケージの否定キーの両方によって暗号化される段階。

【００２２】

本方法の特殊性は、サブスクリプションパッケージのための２つのキーマテリアルを規定することである。受信器が前記サブスクリプションパッケージに対して許可されるときに、このキーのうちの１つ（肯定キーマテリアル）はロードされ、他方（否定キーマテリアル）は前記サブスクリプションパッケージにアクセスしない受信器にロードされる。

【００２３】

管理センターは最初に属性（例えば、サービス又はサブスクリプションパッケージのセット）を対象とし、考えられる属性をリストし、属性ごとに、キーマテリアルが決定される。キーマテリアルによって、それは少なくともこの属性及び任意に権利定義に関連したキーを意味する。

【００２４】

本発明は、第１サブスクリプションパッケージを受ける権利があるが、第２サブスクリプションパッケージを受ける権利がない特定の受信装置の場合は、前記受信装置は第１サブスクリプションパッケージの肯定キーマテリアル及び第２サブスクリプションパッケージの否定マテリアルを受け取るという事実に基づいている。

【００２５】

このキーマテリアルのおかげで、受信装置に第１サブスクリプションパッケージの資格があるが、第２サブスクリプションパッケージの資格がない場合に限り、キーメッセージは番組キーへのアクセスを可能にするような複雑な問合わせを伝えることができる。

【００２６】

受信キー又は番組キーは、即ちセキュリティモジュール内の更なるキー又はアルゴリズムを用いて番組を直接受信するか又は番組を間接的に受信するために使用できる。この受信キーは、同じメッセージ又は特許文献２に記載されたような他の資格管理メッセージの他のキーと組み合わすことができ、受信キーはこのケースにおいてマスターキーの役割を果たす。

【００２７】

他の実施形態では、受信キーは、制御ワード及び受信条件を含むメッセージを暗号化する（又は、復号する）ために用いる、いわゆる伝達キーである。

【図面の簡単な説明】

【００２８】

本発明は、放送環境の概略が例示される添付図の助けを借りて説明される。

【発明を実施するための形態】

【００２９】

新しい加入者の初期設定中に、その受信器のセキュリティモジュールは、このユーザ専用であるキーマテリアルを含むメッセージを受信する。

【００３０】

管理センターが４つのサブスクリプションパッケージ（各パッケージは少なくとも１つのオーディオ／ビデオ・サービスを含む）を管理し、複数のサービスを含むことができる実施例を挙げる。このユーザが第１サブスクリプションパッケージを契約したという場合において、第１サブスクリプションパッケージの肯定キーマテリアルは、そのセキュリティモジュールに記憶するために受信器に送られる。管理センターはまた、加入者が受信できない他のサブスクリプションパッケージの否定キーマテリアルも送信する。

【００３１】

この構造のおかげで、肯定及び否定キーマテリアルを使用して特定の放送番組に対する

受信条件を規定することが、現在可能である。第１パッケージに対する契約をしたが、第２パッケージに対する契約をしなかった加入者が番組を受信できる実施例によれば、番組キー、即ち番組を復号するためのキーは、従って、第１サブスクリプションパッケージの肯定キーによって、また再び、第２サブスクリプションパッケージの否定キーによって暗号化される。メッセージはこの二重暗号化された番組キーにより形成されて加入者に送られる。そして第１パッケージを受信できるが、第２パッケージを受信できない我々の特定の加入者は、この二重暗号化された番組キーを復号できる。別の加入者が第１及び第２のパッケージを受信するという場合に、前記加入者は第２サブスクリプションパッケージの否定キーを持たず、番組キーを復号することができないだろう。

【００３２】

従って番組に対する受信条件は管理センターにより施行されて、加入者のユニットによってなされる検証に依存しない。

【００３３】

暗号化の順序、即ち、肯定キー及び次に否定キーが因果関係なしで逆にされることがある。否定キーは最初に使用でき、肯定キーはその後に使用できる。

【００３４】

受信条件が第３サブスクリプションパッケージに影響を与えるはずである場合には、番組キーは、状態が第３サブスクリプションパッケージを受信できるか、又は受信できないという事実に応じて、第３サブスクリプションパッケージの肯定又は否定キーによって更に暗号化され得る。

【００３５】

本発明の実施形態によれば、番組キーはまず最初にセッションキーによって暗号化される。これは肯定及び否定キーを取扱うためのより柔軟な方法を可能にする。肯定及び否定キーが非対称のキーであるという場合には、非対称のキーによる暗号化されたマテリアルのサイズは非対称のアルゴリズムにより規定される。これはセッションキーのサイズのみに影響を与え、番組キーのサイズを開いたままにする。９６ビットの番組キーが使用でき、１２８ビットのセッションキーによって暗号化できる。セッションキーは、その後で、上記の通りに番組キーの代わりに受信条件に従って暗号化される。加入者のユニットに送られるメッセージは、セッションキーによって暗号化される番組キー、及びサブスクリプションパッケージの受信条件に従って肯定又は否定キーによって暗号化されるセッションキーを含む。

【００３６】

加入者がその契約を変更できるので、本発明の一実施形態によれば、肯定及び否定キーマテリアルは定期的に、例えば毎月更新される。そのため、加入者がこのパッケージを契約するときに、彼は所与のサブスクリプションパッケージの否定キーを持ち続けることに関心を有しない。管理センターは、この加入者に、彼が受ける権利があるサブスクリプションパッケージの来月分の新しい肯定キー、及び彼が受ける権利がないサブスクリプションパッケージの来月分の新しい否定キーを送る。このため、加入者ユニットの格納手段に前月の管理を保つことは、それが肯定及び否定キーの組合せに基づいて受信条件を回避するのを不可能にする。

【００３７】

図１において、管理センターＭＣは、受信装置ＲＤ１、ＲＤ２、ＲＤ３において送られるキーマテリアルのコピーをそのデータベースＤＢに格納する。我々の実施例によれば、２つのサブスクリプションパッケージＢ１、Ｂ２が規定され、第１のものは肯定キーマテリアルＫ１及び否定マテリアルＫ１´に関連し、第２のものは肯定キーマテリアルＫ２及び否定マテリアルＫ２´に関連している。

【００３８】

サブスクリプションパッケージＢ１を受ける権利がある受信装置ＲＤ１は、キーマテリアルＫ１を受信した。この受信装置ＲＤ１がサブスクリプションパッケージＢ２を受ける権利がないという事実のため、キーマテリアルＫ２´はそれにも送信された。

【００３９】
受信装置ＲＤ２はサブスクリプションパッケージＢ１及びＢ２を受ける権利があり、キーマテリアルＫ１及びＫ２は両方共この装置に送られた。
【００４０】
受信装置ＲＤ２はサブスクリプションパッケージＢ２を受ける権利があり、キーマテリアルＫ２がそれに送られた。この受信装置ＲＤ３がサブスクリプションパッケージＢ１を受ける権利がないという事実のため、キーマテリアルＫ１´はそれにも送信された。
【００４１】
管理センターＭＣが、第２サブスクリプションパッケージＢ２に許可され第１サブスクリプションパッケージＢ１に許可されない受信装置のみに受信キーＫを送る必要があるという場合には、受信装置ＲＤに送られる暗号ＣＹは、否定キーマテリアルＫ１´及び肯定キーマテリアルＫ２と組み合わされた受信キーを含む。
【００４２】
暗号を含む許可メッセージにおいて、メッセージの別のフィールドは復号の用に供するキーの記述子を含む。これは２つのビットマップの形とすることができ、各アクティブビットはサブスクリプションパッケージを規定し、１つのビットマップは肯定キーに関するものであり、他のものは否定キーに関するものである。本発明の実施態様によれば、それは、肯定キーが暗号を復号するために最初に使用され、次に否定キーが使用されることを決定することができた。
【００４３】
番組キーは、単一の放送番組例えば映画を解除できるか、あるいは１日又は１ヵ月のサービスを解除できる。
【００４４】
サブスクリプションパッケージは複数のサービス又は単一のサービスに関連できる。このように、本発明は、チャネル３（第１サブスクリプションパッケージ）及びチャネル６なし（第２サブスクリプションパッケージ）の受信を組み合わせることによって、この番組製品の受信規則を規定することを可能にする。

【図１】

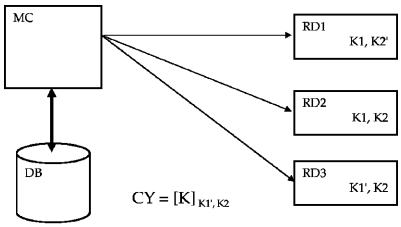

Fig. 1

フロントページの続き

(56)参考文献 特開２００７－２５１９１３（ＪＰ，Ａ）
国際公開第２００６／０５５８５３（WO，Ａ２）
米国特許出願公開第２００８／０１９２９３６（ＵＳ，Ａ１）
米国特許出願公開第２００８／００１９５１７（ＵＳ，Ａ１）
米国特許出願公開第２００６／０１８４７９６（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１６８０６３（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 7/173
H04H 60/16
H04H 60/23