(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2008-521275
(P2008-521275A)
(43)公表日　平成20年6月19日(2008.6.19)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5C164
H04N	7/173	(2006.01)	H04N	7/173	630	5J104
H04N	7/167	(2006.01)	H04N	7/167	Z	
			H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 19 頁）

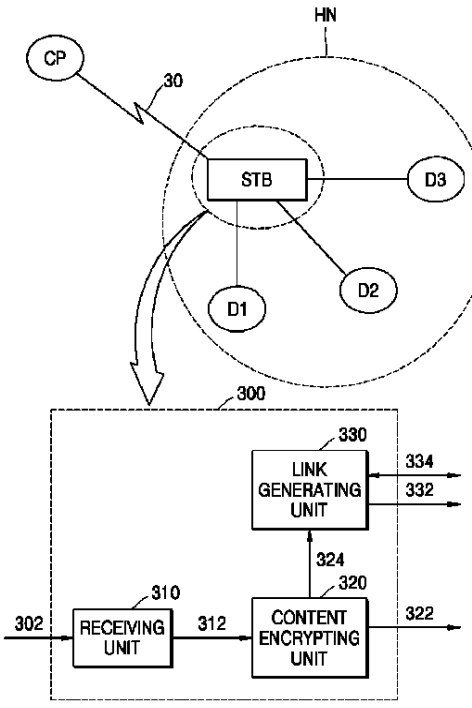
(21)出願番号　特願2007-541095 (P2007-541095)
(86)(22)出願日　平成17年11月8日 (2005.11.8)
(85)翻訳文提出日　平成19年5月10日 (2007.5.10)
(86)国際出願番号　PCT/KR2005/003766
(87)国際公開番号　WO2006/054844
(87)国際公開日　平成18年5月26日 (2006.5.26)
(31)優先権主張番号　60/627,967
(32)優先日　平成16年11月16日 (2004.11.16)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10-2004-0097998
(32)優先日　平成16年11月26日 (2004.11.26)
(33)優先権主張国　韓国 (KR)

(71)出願人　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(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　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】放送コンテンツの受信装置及び方法

(57)【要約】
放送コンテンツを受信する装置において、ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成する受信部と、ｂ）所定のコンテンツキーを利用してコンテンツを暗号化するコンテンツ暗号化部と、ｃ）コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、ユーザ機器との安全なリンクを生成し、安全なリンクを通じてコンテンツキーをユーザ機器に伝送するリンク生成部と、を備え、リンクメッセージのうち、第１リンクメッセージは、ユーザ機器の公開キー及び放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、放送受信装置の個人キー、秘密キー及びユーザ機器の秘密キーのうち一つを含む装置である。



【特許請求の範囲】
【請求項１】
放送コンテンツを受信する装置において、
ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成する受信部と、
ｂ）所定のコンテンツキーを利用して、前記コンテンツを暗号化するコンテンツ暗号化部と、
ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、前記ユーザ機器との安全なリンクを生成し、前記安全なリンクを通じて前記コンテンツキーをユーザ機器に伝送するリンク生成部と、を備え、
前記リンクメッセージのうち、第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含むことを特徴とする装置。
【請求項２】
前記ｃ）リンク生成部は、
前記ユーザ機器からのリンク要請メッセージをカウントし、現在リンク数を最大リンク数と比較することによって、前記現在リンクの回数を制限することを特徴とする請求項１に記載の装置。
【請求項３】
ｃ）前記リンク生成部は、
前記ユーザ機器の公開キーを利用して前記受信装置の個人キーを暗号化した後に、前記ユーザ機器に伝送し、
前記受信装置の公開キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。
【請求項４】
ｃ）前記リンク生成部は、
前記ユーザ機器の公開キーを利用して前記受信装置の秘密キーを暗号化した後に、前記ユーザ機器に伝送し、
前記受信装置の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。
【請求項５】
ｃ）前記リンク生成部は、
前記受信装置の公開キーを利用して暗号化された前記ユーザ機器の秘密キーを受信し、
前記受信されたユーザ機器の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。
【請求項６】
放送コンテンツを受信する方法において、
ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成するステップと、
ｂ）所定のコンテンツキーを利用して前記コンテンツを暗号化するコンテンツ暗号化ステップと、
ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、前記ユーザ機器との安全なリンクを生成し、前記安全なリンク

を通じて前記コンテンツキーをユーザ機器に伝送するリンク生成ステップと、を含み、
前記リンクメッセージのうち第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含むことを特徴とする方法。
【請求項７】
前記ｃ）リンク生成ステップは、
前記ユーザ機器からのリンク要請メッセージをカウントすることによって現在リンク数を生成するステップと、
現在リンク数を最大リンク数と比較することによって、前記現在リンクの回数を制限するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項８】
ｃ）前記リンク生成ステップは、
前記ユーザ機器の公開キーを利用して前記受信装置の個人キーを暗号化した後に、前記ユーザ機器に伝送するステップと、
前記受信装置の公開キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項９】
ｃ）前記リンク生成ステップは、
前記ユーザ機器の公開キーを利用して前記受信装置の秘密キーを暗号化した後に、前記ユーザ機器に伝送するステップと、
前記受信装置の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項１０】
ｃ）前記リンク生成ステップは、
前記受信装置の公開キーを利用して暗号化された前記ユーザ機器の秘密キーを受信するステップと、
前記受信されたユーザ機器の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項１１】
請求項６に記載の方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、放送コンテンツの受信装置及び方法に係り、さらに詳細には、コンテンツ提供者と連結されていないオフライン状態でも放送コンテンツを安定的にユーザ機器に伝送可能な放送受信装置及び方法に関する。
【背景技術】
【０００２】
デジタルコンテンツは、コンテンツ提供者からユーザに伝送される。ユーザは、コンテンツに対するコストの支払を通じて正当な権限を獲得して初めて、デジタルコンテンツを使用でき、また、正当な権限を獲得していないユーザは、デジタルコンテンツを使用できないように、コンテンツは保護されねばならない。
【０００３】
正当な権限のないユーザにとってコンテンツを獲得することを防止するために、コンテンツは、コンテンツキーで暗号化され、コンテンツキーは、正当な権限のあるユーザにのみ配布される。
【０００４】

一方、最近、ホームネットワーク技術の発達によって、１人のユーザが一つ以上のユーザ機器を所有し、また、これらの間にコンテンツの移動が可能になった。ユーザは、一回のコスト決済で自身が所有した全ての機器に対してコンテンツを使用することを所望する。しかし、コンテンツが機器の間で再生できる形態で自由に移動可能であれば、権限のないユーザがコンテンツを獲得して使用しうる。したがって、ホームネットワーク技術では、権限のあるユーザのホームネットワーク内のユーザ機器の間には、コンテンツの移動を許容しつつ、権限のないユーザは、コンテンツが獲得できないか、または獲得するとしても、コンテンツが使用できないようにする技術が必要である。

【０００５】

図１は、インターネットを通じたコンテンツの受信方法を示す図面である。

【０００６】

コンテンツ提供者ＣＰは、インターネット１０を通じてユーザ機器Ｄ１，Ｄ２，Ｄ３にコンテンツを伝送する。コンテンツ提供者ＣＰとユーザ機器Ｄ１，Ｄ２，Ｄ３とは、インターネットを通じて連結されているので、ユーザ機器とコンテンツ提供者との間に双方向通信が可能である。

【０００７】

ユーザ機器Ｄ１，Ｄ２，Ｄ３とコンテンツ提供者ＣＰとの間に双方向通信が可能であるため、コンテンツ提供者ＣＰとユーザ機器Ｄ１，Ｄ２，Ｄ３とが正当な権限を有しているか否かを判断するユーザ認証、暗号化されたコンテンツの伝送及びコンテンツキーの伝送などのコンテンツ保護のための一連の過程が具現可能である。

【０００８】

このようなユーザ機器Ｄ１，Ｄ２，Ｄ３がユーザＵのホームネットワークＨＮに続属すれば、ユーザＵは、他の権限のないユーザから安全に自身のみのユーザ機器Ｄ１，Ｄ２，Ｄ３でコンテンツを使用しうる。

【０００９】

図２は、放送を通じたコンテンツの受信方法を示す図面である。

【００１０】

コンテンツ提供者ＣＰは、放送チャンネル２０を通じてユーザ機器Ｄ１，Ｄ２，Ｄ３にコンテンツを伝送する。一般的に、コンテンツは、セットップボックスと呼ばれるデジタル放送受信機１２から受信した後に、ユーザ機器Ｄ１，Ｄ２，Ｄ３に伝送される。

【００１１】

放送の特徴によって、コンテンツ提供者ＣＰは、公衆を通じて一方的にコンテンツをユーザ機器Ｄ１，Ｄ２，Ｄ３に伝送するので、ユーザ機器とコンテンツ提供者との間に双方向通信が不可能である。

【００１２】

ユーザ機器Ｄ１，Ｄ２，Ｄ３とコンテンツ提供者ＣＰとの間に双方向通信が不可能であるため、コンテンツ提供者ＣＰは、ユーザ機器Ｄ１，Ｄ２，Ｄ３が正当な権限を有しているか否かを判断するユーザ認証、暗号化されたコンテンツの伝送及びコンテンツキーの伝送などのコンテンツ保護のための一連の過程に対する具現が不可能である。

【００１３】

したがって、前述したユーザ認証のようなコンテンツ保護の過程は、デジタル放送を受信するシナリオでは適用不可能である。すなわち、セットップボックスは、一般的に所定の放送プロトコルによってデジタル放送を受信し、受信されたコンテンツをユーザＵのホームネットワークＨＮに属するユーザ機器Ｄ１，Ｄ２，Ｄ３にのみ伝送するため、他の権限のないユーザがコンテンツを獲得することが防止できない。

【００１４】

特に、米連邦通信委員会（ＦＣＣ：Ｆｅｄｅｒａｌ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｃｏｍｍｉｓｓｉｏｎ）は、２００５年７月から米国内のデジタル放送で放送される高画質のＨＤ級コンテンツに対して１ビットのブロードキャストフラッグ（ＢＦ）を添加し、該当コンテンツのブロードキャストフラッグが１である場合には、コンテンツ保護がなされ

るように、すなわち、権限のないユーザの使用を防止する技術をデジタル放送具現技術標準で要求しているため、コンテンツ提供者とユーザ機器とで双方向通信が不可能である、すなわち、インターネットで連結されていないオフライン状態でも、デジタル放送コンテンツの安全な使用に対する要求はさらに切実である。

【発明の開示】

【発明が解決しようとする課題】

【００１５】

本発明は、前述した課題を解決するために案出されたものであって、コンテンツ提供者とユーザ機器との間に双方向通信が不可能な状況でも、正当なユーザのユーザ機器は、コンテンツを再生可能にすると同時に、正当な権限のない他のユーザは、該当コンテンツを再生不可能にする放送コンテンツの受信装置及び方法を提供することを目的とする。

【課題を解決するための手段】

【００１６】

前記目的を解決するための本発明は、放送コンテンツを受信する装置において、ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成する受信部と、ｂ）所定のコンテンツキーを利用して前記コンテンツを暗号化するコンテンツ暗号化部と、ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、前記ユーザ機器との安全なリンクを生成し、前記安全なリンクを通じて前記コンテンツキーをユーザ機器に伝送するリンク生成部と、を備え、前記リンクメッセージのうち、第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含む。

【００１７】

ここで、前記ｃ）リンク生成部は、前記ユーザ機器からのリンク要請メッセージをカウントし、現在リンク数を最大リンク数と比較することによって、前記現在リンクの回数を制限する。

【００１８】

一実施例で、ｃ）前記リンク生成部は、前記ユーザ機器の公開キーを利用して前記受信装置の個人キーを暗号化した後に前記ユーザ機器に伝送し、前記受信装置の公開キーを利用して前記コンテンツキーを暗号化した後に前記ユーザ機器に伝送することによって、前記コンテンツキーを前記ユーザ機器に伝送する。

【００１９】

他の実施例で、ｃ）前記リンク生成部は、前記ユーザ機器の公開キーを利用して前記受信装置の秘密キーを暗号化した後に前記ユーザ機器に伝送し、前記受信装置の秘密キーを利用して前記コンテンツキーを暗号化した後に前記ユーザ機器に伝送することによって、前記コンテンツキーを前記ユーザ機器に伝送する。

【００２０】

さらに他の実施例で、ｃ）前記リンク生成部は、前記受信装置の公開キーを利用して暗号化された前記ユーザ機器の秘密キーを受信し、前記受信されたユーザ機器の秘密キーを利用して前記コンテンツキーを暗号化した後に前記ユーザ機器に伝送することによって、前記コンテンツキーを前記ユーザ機器に伝送する。

【００２１】

また、本発明は、放送コンテンツを受信する方法において、ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成するステップと、ｂ）所定のコンテンツキーを利用して前記コンテンツを暗号化するコンテンツ暗号化ステップと、ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、前記ユーザ機器との安全なリンクを生成し、前記安全なリンクを通じて前記コンテンツキーをユーザ機器に伝送するリンク生成ステップと、を含み、前記リンクメッセージのうち第１リンクメッセージは、前記ユーザ機器の公

開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含む。

【発明の効果】

【００２２】

本発明によれば、放送受信装置とユーザ機器との間に安全なリンクが形成されることによって、コンテンツ提供者とユーザ機器とが連結されていない状況でもコンテンツが安全にユーザ機器に伝送される。

【００２３】

また、本発明によれば、放送受信装置でリンク可能な回数を制限することによって無制限的なコンテンツの使用を防止しうる。

【００２４】

また、本発明によれば、米連邦通信委員会が２００５年７月にＨＤ級コンテンツに要求するブロードキャストフラッグの具現によって容易に適用されうる放送受信装置が提供される。

【発明を実施するための最良の形態】

【００２５】

以下、添付された図面を参照して本発明による望ましい一実施例を詳細に説明する。

【００２６】

図３は、本発明による放送受信装置を示す図面である。

【００２７】

本発明による放送受信装置３００は、受信部３１０、コンテンツ暗号化部３２０及びリンク生成部３３０を備える。

【００２８】

受信部３１０は、放送チャンネル３０から放送ストリーム３０２を受信し、受信された放送ストリーム３０２でユーザの所望するコンテンツに対応するパケットを組合わせることによってコンテンツ３１２を生成する。

【００２９】

コンテンツ暗号化部３２０は、所定のコンテンツキー３２４を利用してコンテンツ３１２を暗号化することによって、暗号化されたコンテンツ３２２を生成する。コンテンツキー３２４は、コンテンツ暗号化部３２０内で生成されてもよく、外部で生成されてコンテンツ暗号化部３２０に供給されてもよい。いかなる場合でも、コンテンツキーは、正当な権限を有するユーザのみが獲得可能でなければならない。コンテンツキー３２４がコンテンツ暗号化部３２０内で生成される場合には、例えば、乱数生成を通じて生成可能である。コンテンツキー３２４は、リンク生成部３３０を通じて安全な状態でユーザ機器に伝送される。

【００３０】

リンク生成部３３０は、ユーザ機器とリンクメッセージ３３４を交換することによって、ユーザ機器との安全なリンクを生成し、生成された安全なリンクを通じて、暗号化されたコンテンツキー３２４をユーザ機器に伝送する。

【００３１】

安全なリンクとは、放送受信装置ＳＴＢとユーザ機器Ｄ１，Ｄ２，Ｄ３との間にコンテンツキーを伝送するための経路であって、放送受信装置とユーザ機器以外の機器とは、コンテンツキーを獲得不可能にする経路を意味する。ユーザ機器とリンク生成部との間に行われるリンクメッセージの交換は、図５ないし図７を利用してさらに詳細に説明する。

【００３２】

また、リンクメッセージのうち、第１リンクメッセージは、ユーザ機器の公開キー及び放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、放送受信装置の個人キー、秘密キー及びユーザ機器の秘密キーのうち一つを含みうる。

【００３３】

変形された実施例で、リンク生成部３３０は、リンク生成の数をカウントすることによ

って放送受信装置ＳＴＢに連結されるユーザ機器の数を制限可能である。
【００３４】
図４は、本発明によるユーザ機器の構成を示す図面である。
【００３５】
本発明による放送受信装置からコンテンツを受信して再生するためのＤ１，Ｄ２，Ｄ３等ユーザー機器４００は、コンテンツ復号化部４１０、キー生成部４２０及び再生部４３０を備える。
【００３６】
コンテンツ復号化部４１０は、放送受信装置ＳＴＢ、例えば、図３の放送受信装置３００のコンテンツ暗号化部３２０から暗号化されたコンテンツ４０２を受信し、コンテンツキー４２６を利用して暗号化されたコンテンツ４０２を復号化することによって、復号化されたコンテンツ４１２を生成する。コンテンツキー４２６は、キー生成部４２０から提供される。
【００３７】
キー生成部４２０は、放送受信装置ＳＴＢとリンクメッセージ４０４を交換することによって、放送受信装置ＳＴＢ、例えば、図３の放送受信装置３００のリンク生成部３３０から暗号化されたコンテンツキー３３２を受信する。ユーザ機器とリンク生成部との間に行われるリンクメッセージの交換は、図５ないし図７を利用してさらに詳細に説明する。
【００３８】
図５ないし図７は、放送受信装置のリンク生成部がリンクメッセージ交換を通じてリンクを生成するコンテンツキーをユーザ機器に伝送する方法の例を示す図面である。
【００３９】
図５は、本発明の第１実施例によるリンク生成部のリンク生成方法を示す図面である。
【００４０】
ステップ５１０で、放送受信装置３００のリンク生成部３３０（以下、リンク生成部という）は、ユーザ機器４００のキー生成部４２０（以下、キー生成部という）から、リンクを要請するリンク要請メッセージＲｅｑｕｅｓｔ及び公開キーＫｐｕｂ＿ｄｅｖを受信する。
【００４１】
ステップ５１５で、リンク生成部３３０は、現在リンク数Ｎより最大リンク数Ｎｃが大きいか否かを判断し、もし、大きければ、ステップ５２０に進み、そうでなければ、ステップ５８０で該当ユーザ機器からのリンク要請を拒否する拒否メッセージをユーザ機器に伝送することによって、リンクを拒否する。
【００４２】
ステップ５２０で、リンク生成部３３０は、ステップ５１０で受信した機器４００の公開キーＫｐｕｂ＿ｄｅｖを利用して放送受信装置３００の個人キーＫｐｒｉ＿ＳＴＢを暗号化することによって、暗号化された放送受信装置の個人キーＥ１＝Ｅ（Ｋｐｕｂ＿ｄｅｖ，Ｋｐｒｉ＿ＳＴＢ）を生成した後にキー生成部４２０に伝送する。
【００４３】
ステップ５３０で、キー生成部４２０は、ユーザ機器の個人キーＫｐｒｉ＿ｄｅｖを利用して、ステップ５２０で受信した暗号化された放送受信装置の個人キーＥ１を復号化することによって、放送受信装置の個人キーＫｐｒｉ＿ＳＴＢを生成する。
【００４４】
ステップ５４０で、リンク生成部３３０は、放送受信装置の公開キーＫｐｕｂ＿ＳＴＢを利用してコンテンツキーＫ＿ｃｏｎｔを暗号化することによって、暗号化されたコンテンツキーＥ２＝Ｅ（Ｋｐｕｂ＿ＳＴＢ，Ｋ＿ｃｏｎｔ）を生成した後にキー生成部４２０に伝送する。
【００４５】
ステップ５５０で、キー生成部５５０は、ステップ５３０で生成した放送受信装置の個人キーＫｐｒｉ＿ＳＴＢを利用してステップ５４０で受信した暗号化されたコンテンツキ

ーＥ２を復号化することによって、コンテンツキーＫ＿ｃｏｎｔを生成する。
【００４６】
ステップ５６０で、キー生成部５５０は、コンテンツキーが成功的に生成されたことを表す成功メッセージｓｕｃｃｅｓｓをリンク生成部３３０に伝送する。
【００４７】
ステップ５７０で、リンク生成部３３０は、現在リンク数Ｎに１を追加することによって現在リンク数を更新し、再びステップ５１０に進む。
【００４８】
図５の実施例によれば、公開キーの構造を利用して、コンテンツキーは、放送受信装置からユーザ機器に安全に伝送される。言い換えれば、コンテンツキーは、ユーザ機器の個人キー、ユーザ機器の公開キー、放送受信装置の個人キー及び放送受信装置の公開キーを利用して安全に伝送される。外部機器は、ステップ５１０、５２０、５４０でのリンクメッセージをハッキングしても、全てのリンクメッセージは、暗号化された状態であるので、コンテンツキーが生成できないので、結局、放送受信装置は、コンテンツキーを安全なリンクを通じてユーザ機器に伝送可能である。
【００４９】
また、このような方法によれば、放送受信装置は、コンテンツ提供者とのオフライン状態でもユーザ機器にコンテンツを安全に伝送できて、前述した米連邦通信委員会で規定するブロードキャストフラッグの要求事項を満足させうる。
【００５０】
また、図５の実施例で、ステップ５１５、５６０、５７０及び５８０は、省略可能である。ステップ５１５、５６０、５７０、５８０が追加されることによって、放送受信装置の製造者は、一つの放送受信装置で再生可能な回数を制限可能であり、これは、ユーザが放送受信装置を通じて不法的な方法でコンテンツを流布することを防止しうる。
【００５１】
図６は、本発明の第２実施例によるリンク生成部のリンク生成方法を示す図面である。
【００５２】
ステップ６１０で、放送受信装置３００のリンク生成部３３０（以下、リンク生成部という）は、ユーザ機器４００のキー生成部４２０（以下、キー生成部という）から、リンクを要請するリンク要請メッセージＲｅｑｕｅｓｔ及び公開キーＫｐｕｂ＿ｄｅｖを受信する。
【００５３】
ステップ６１５で、リンク生成部３３０は、現在リンク数Ｎより最大リンク数Ｎｃが大きいか否かを判断し、もし、大きければ、ステップ６２０に進み、そうでなければ、ステップ６８０で該当ユーザ機器からのリンク要請を拒否する拒否メッセージをユーザ機器に伝送することによって、リンクを拒否する。
【００５４】
ステップ６２０で、リンク生成部３３０は、ステップ６１０で受信したユーザ機器４００の公開キーＫｐｕｂ＿ｄｅｖを利用して放送受信装置３００の秘密キーＫｓｅｃ＿ＳＴＢを暗号化することによって、暗号化された放送受信装置の秘密キーＥ１＝Ｅ（Ｋｐｕｂ＿ｄｅｖ，Ｋｓｅｃ＿ＳＴＢ）を生成した後に、キー生成部４２０に伝送する。
【００５５】
ステップ６３０で、キー生成部４２０は、ユーザ機器の個人キーＫｐｒｉ＿ｄｅｖを利用してステップ６２０で受信した暗号化された放送受信装置の秘密キーＥ１を復号化することによって、放送受信装置の秘密キーＫｓｅｃ＿ＳＴＢを生成する。
【００５６】
ステップ６４０で、リンク生成部３３０は、放送受信装置の秘密キーＫｓｅｃ＿ＳＴＢを利用してコンテンツキーＫ＿ｃｏｎｔを暗号化することによって、暗号化されたコンテンツキーＥ２＝Ｅ（Ｋｓｅｃ＿ＳＴＢ，Ｋ＿ｃｏｎｔ）を生成した後に、キー生成部４２０に伝送する。

【００５７】
ステップ６５０で、キー生成部６５０は、ステップ６３０で生成した放送受信装置の秘密キーＫｓｅｃ＿ＳＴＢを利用してステップ６４０で受信した暗号化されたコンテンツキーＥ２を復号化することによって、コンテンツキーＫ＿ｃｏｎｔを生成する。
【００５８】
ステップ６６０で、キー生成部６５０は、コンテンツキーが成功的に生成されたことを表す成功メッセージｓｕｃｃｅｓｓをリンク生成部３３０に伝送する。
【００５９】
ステップ６７０で、リンク生成部３３０は、現在リンク数Ｎに１を追加することによって現在リンク数を更新し、再びステップ６１０に進む。
【００６０】
図６の実施例によれば、ユーザ機器の個人キー、ユーザ機器の公開キー、及び放送受信装置の秘密キーを利用して、コンテンツキーは、安全に伝送される。コンテンツキーが対称する構造を利用して放送受信装置からユーザ機器に伝送されるという点で、図５の実施例と相異なる。図５と同様に、外部機器は、ステップ６１０、６２０、６４０でのリンクメッセージをハッキングしても、全てのリンクメッセージは、暗号化された状態であるので、コンテンツキーを生成できないので、結局、放送受信装置は、コンテンツキーを安全なリンクを通じてユーザ機器に伝送可能である。
【００６１】
また、図５と同様に、ステップ６１５、６６０、６７０及び６８０は、省略可能である。
【００６２】
図７は、本発明の第３実施例によるリンク生成部のリンク生成方法を示す図面である。
【００６３】
ステップ７１０で、放送受信装置３００のリンク生成部３３０（以下、リンク生成部という）は、ユーザ機器４００のキー生成部４２０（以下、キー生成部という）から、リンクを要請するリンク要請メッセージＲｅｑｕｅｓｔを受信する。
【００６４】
ステップ７１５で、リンク生成部３３０は、現在リンク数Ｎより最大リンク数Ｎｃが大きいか否かを判断し、もし、大きければ、ステップ７２０に進み、そうでなければ、ステップ７８０で該当ユーザ機器からのリンク要請を拒否する拒否メッセージをユーザ機器に伝送することによって、リンクを拒否する。
【００６５】
ステップ７２０で、リンク生成部３３０は、放送受信装置の公開キーＫｐｕｂ＿ＳＴＢをユーザ機器のキー生成部４２０に伝送する。
【００６６】
ステップ７２５で、キー生成部４２０は、ステップ７２０で受信した放送受信装置３００の公開キーＫｐｕｂ＿ＳＴＢを利用してユーザ機器の秘密キーＫｓｅｃ＿ｄｅｖを暗号化することによって、暗号化されたユーザ機器の秘密キーＥ１＝Ｅ（Ｋｐｕｂ＿ｄｅｖ，Ｋｐｒｉ＿ＳＴＢ）を生成した後にリンク生成部３３０に伝送する。
【００６７】
ステップ７３０で、リンク生成部３３０は、放送受信装置の個人キーＫｐｒｉ＿ＳＴＢを利用してステップ７２５で受信した暗号化されたユーザ機器の秘密キーＥ１を復号化することによって、ユーザ機器の秘密キーＫｓｅｃ＿ｄｅｖを生成する。
【００６８】
ステップ７４０で、リンク生成部３３０は、ステップ７３０で生成されたユーザ機器の秘密キーＫｓｅｃ＿ｄｅｖを利用してコンテンツキーＫ＿ｃｏｎｔを暗号化することによって、暗号化されたコンテンツキーＥ２＝Ｅ（Ｋｓｅｃ＿ｄｅｖ，Ｋ＿ｃｏｎｔ）を生成した後に、キー生成部４２０に伝送する。
【００６９】

ステップ７５０で、キー生成部４２０は、ユーザ機器の秘密キーＫｓｅｃ＿ｄｅｖを利用してステップ７４０で受信した暗号化されたコンテンツキーＥ２を復号化することによって、コンテンツキーＫ＿ｃｏｎｔを生成する。

【００７０】

ステップ７６０で、キー生成部４２０は、コンテンツキーが成功的に生成されたことを表す成功メッセージｓｕｃｃｅｓｓをリンク生成部３３０に伝送する。

【００７１】

ステップ７７０で、リンク生成部３３０は、現在リンク数Ｎに１を追加することによって現在リンク数を更新し、再びステップ７１０に進む。

【００７２】

図７の実施例によれば、コンテンツキーは、ユーザ機器の秘密キーを利用して暗号化される。ユーザの秘密キーは、ユーザごとに固有に割当てられ、公開されていないキーである。図５及び図６の実施例と同様に、外部機器は、ステップ７１０、７２０、７４０でのリンクメッセージをハッキングしても、全てのリンクメッセージは、暗号化された状態であるので、コンテンツキーを生成できないので、結局、放送受信装置は、コンテンツキーを安全なリンクを通じてユーザ機器に伝送可能である。

【００７３】

図５及び図６の実施例と同様に、ステップ７１５、７６０、７７０及び７８０は、省略可能である。

【００７４】

図８は、本発明による放送コンテンツの受信方法を示す図面である。

【００７５】

ステップ８１０で、放送受信装置は、放送チャンネルから放送ストリームを受信し、放送ストリームからコンテンツを生成する。

【００７６】

ステップ８２０で、放送受信装置は、所定のコンテンツキーを利用してステップ８１０で生成されたコンテンツを暗号化した後にユーザ機器に伝送する。

【００７７】

ステップ８３０で、放送受信装置は、リンクメッセージの交換を利用して安全なリンクを生成する。安全なリンクは、図５ないし図７の方法を通じて生成される。

【００７８】

ステップ８４０で、放送受信装置は、ステップ８３０で生成した安全なリンクを通じてステップ８２０の所定のコンテンツキーをユーザ機器に伝送する。

【００７９】

一方、本発明による放送コンテンツの受信方法は、コンピュータプログラムで作成可能である。前記プログラムを構成するコード及びコードセグメントは、当該分野のコンピュータプログラマーによって容易に推論されうる。また、前記プログラムは、コンピュータで読み取り可能な情報記録媒体に保存され、コンピュータによって読み取られ、かつ実行されることによって、放送コンテンツの受信方法を具現する。前記情報記録媒体は、磁気記録媒体、光記録媒体、及びキャリアウェーブ媒体を含む。

【００８０】

以上、本発明についてその望ましい実施例を中心に説明した。当業者は、本発明が本発明の本質的な特性から逸脱しない範囲で変形された形態で具現されうるということが理解できるであろう。したがって、開示された実施例は、限定的な観点ではなく、例示的な観点で考慮されねばならない。本発明の範囲は、前述した説明ではなく、特許請求の範囲に表れており、それと同等な範囲内にある全ての差異点は、本発明に含まれたと解釈されねばならない。

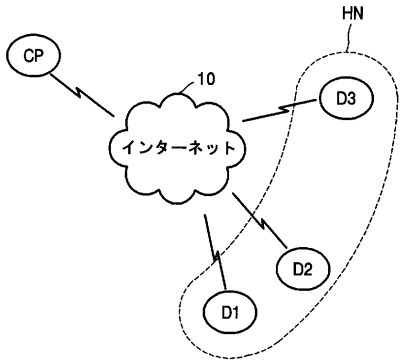
【図面の簡単な説明】

【００８１】

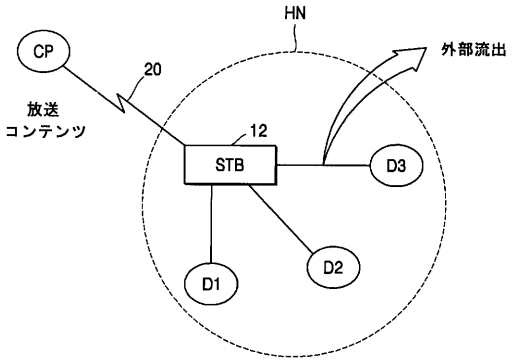
【図１】インターネットを通じたコンテンツの受信方法を示す図面である。

【図２】放送を通じたコンテンツの受信方法を示す図面である。
【図３】本発明による放送受信装置を示す図面である。
【図４】本発明によるユーザ機器の構成を示す図面である。
【図５】本発明の第１実施例によるリンク生成部のリンク生成方法を示す図面である。
【図６】本発明の第２実施例によるリンク生成部のリンク生成方法を示す図面である。
【図７】本発明の第３実施例によるリンク生成部のリンク生成方法を示す図面である。
【図８】本発明による放送コンテンツの受信方法を示す図面である。
【符号の説明】
【００８２】
ＨＮ　ホームネットワーク
ＣＰ　コンテンツ提供者
ＳＴＢ　放送受信装置
３０　放送チャンネル
Ｄ１　ユーザ機器
Ｄ２　ユーザ機器
Ｄ３　ユーザ機器
３００　放送受信装置
３０２　放送ストリーム
３１０　受信部
３１２　コンテンツ
３２０　コンテンツ暗号化部
３２２　暗号化されたコンテンツ
３２４　コンテンツキー
３３０　リンク生成部
３３２　暗号化されたコンテンツキー
３３４　リンクメッセージ

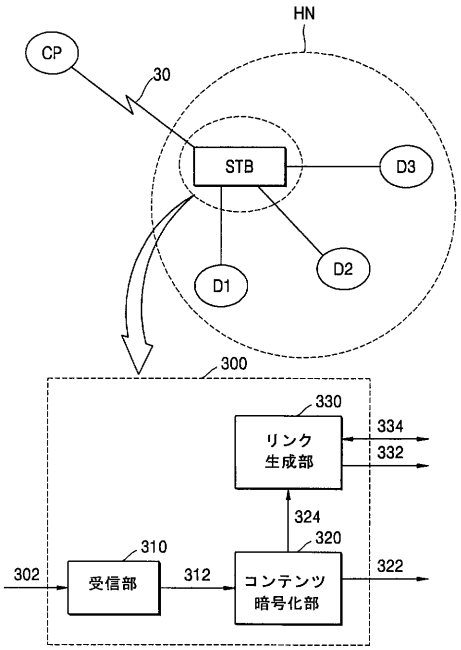
【図１】


HN
CP
10
インターネット
D3
D2
D1

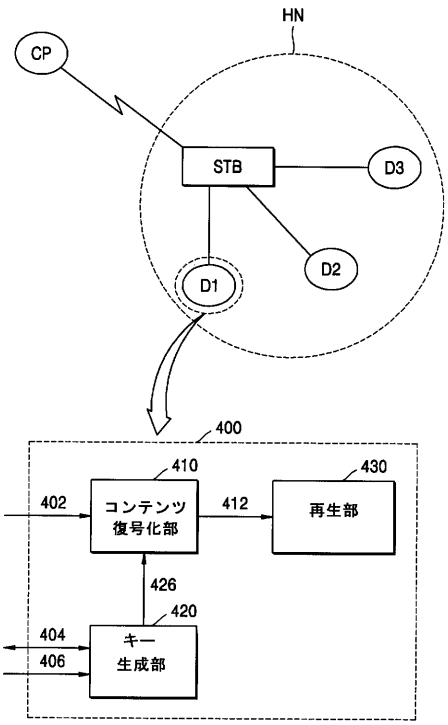
【図２】


HN
CP
放送
コンテンツ
20
外部流出
12
STB
D3
D2
D1

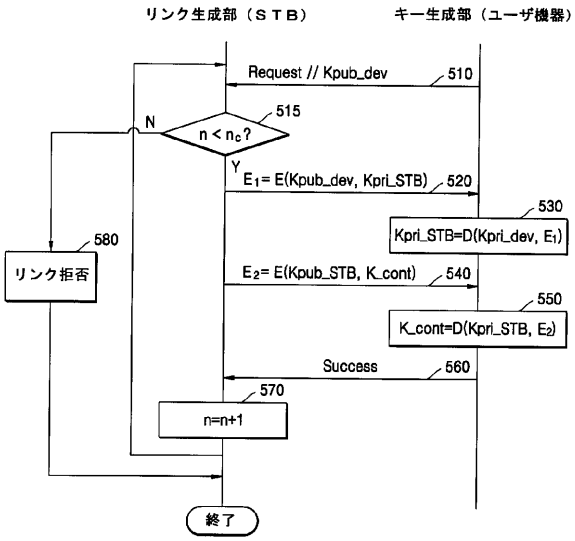
【図３】


HN
CP
30
STB
D3
D2
D1
300
330
リンク
生成部
334
332
324
320
310
302
受信部
312
コンテンツ
暗号化部
322

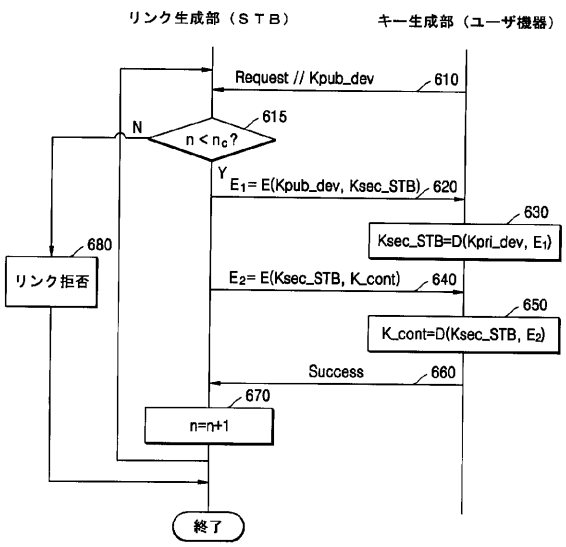
【図４】


HN
CP
STB
D3
D2
D1
400
410
430
402
コンテンツ
復号化部
412
再生部
426
420
404
406
キー
生成部

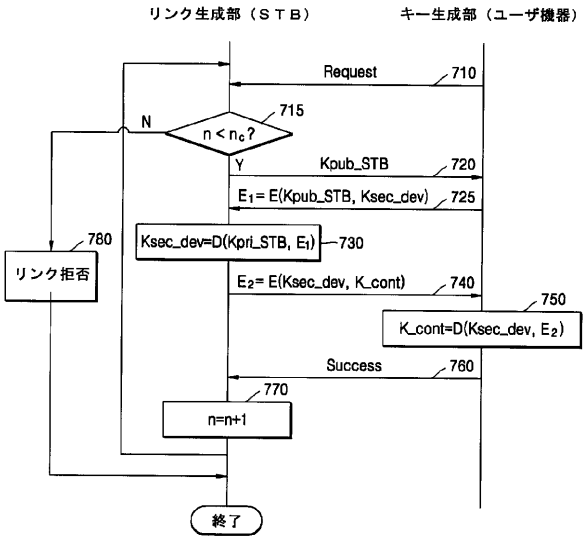
【図５】


リンク生成部（ＳＴＢ）
キー生成部（ユーザ機器）
Request // Kpub_dev
510
515
N
n < nc?
Y
E1= E(Kpub_dev, Kpri_STB)
520
530
Kpri_STB=D(Kpri_dev, E1)
580
リンク拒否
E2= E(Kpub_STB, K_cont)
540
550
K_cont=D(Kpri_STB, E2)
Success
560
570
n=n+1
終了

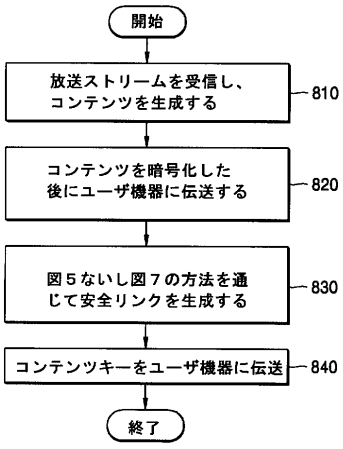
【図６】


リンク生成部（ＳＴＢ）
キー生成部（ユーザ機器）
Request // Kpub_dev
610
615
N
n < nc?
Y
E1= E(Kpub_dev, Ksec_STB)
620
630
Ksec_STB=D(Kpri_dev, E1)
680
リンク拒否
E2= E(Ksec_STB, K_cont)
640
650
K_cont=D(Ksec_STB, E2)
Success
660
670
n=n+1
終了

【図７】


リンク生成部（ＳＴＢ）
キー生成部（ユーザ機器）
Request
710
715
N
n < nc?
Y
Kpub_STB
720
E1= E(Kpub_STB, Ksec_dev)
725
780
Ksec_dev=D(Kpri_STB, E1)
730
リンク拒否
E2= E(Ksec_dev, K_cont)
740
750
K_cont=D(Ksec_dev, E2)
Success
760
770
n=n+1
終了

【図８】


開始
放送ストリームを受信し、
コンテンツを生成する
810
コンテンツを暗号化した
後にユーザ機器に伝送する
820
図５ないし図７の方法を通
じて安全リンクを生成する
830
コンテンツキーをユーザ機器に伝送
840
終了

【手続補正書】
【提出日】平成19年11月16日(2007.11.16)
【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】
放送コンテンツを受信する装置において、
ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成する受信部と、
ｂ）所定のコンテンツキーを利用して、前記コンテンツを暗号化するコンテンツ暗号化部と、
ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器とリンクメッセージを交換することによって、前記ユーザ機器との安全なリンクを生成し、前記コンテンツキーを暗号化するとともに、前記リンクメッセージの１つを介して暗号化された前記コンテンツキーをユーザ機器に伝送するリンク生成部と、を備え、
前記リンクメッセージのうち、第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含むことを特徴とする装置。
【請求項２】
前記ｃ）リンク生成部は、
前記ユーザ機器からのリンク要請メッセージをカウントし、現在リンク数を最大リンク数と比較することによって、前記現在リンクの回数を制限することを特徴とする請求項１に記載の装置。
【請求項３】
ｃ）前記リンク生成部は、
前記ユーザ機器の公開キーを利用して前記受信装置の個人キーを暗号化した後に、前記ユーザ機器に伝送し、
前記受信装置の公開キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。
【請求項４】
ｃ）前記リンク生成部は、
前記ユーザ機器の公開キーを利用して前記受信装置の秘密キーを暗号化した後に、前記ユーザ機器に伝送し、
前記受信装置の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。
【請求項５】
ｃ）前記リンク生成部は、
前記受信装置の公開キーを利用して暗号化された前記ユーザ機器の秘密キーを受信し、
前記受信されたユーザ機器の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送することによって、
前記コンテンツキーを前記ユーザ機器に伝送することを特徴とする請求項１に記載の装置。

【請求項６】
放送コンテンツを受信する方法において、
ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成するステップと、
ｂ）所定のコンテンツキーを利用して前記コンテンツを暗号化するコンテンツ暗号化ステップと、
ｃ）前記コンテンツ提供者と連結されていない状態で、ユーザ機器と放送受信装置との間でリンクメッセージを交換することによって、前記ユーザ機器と前記放送受信装置との間の安全なリンクを生成し、前記コンテンツキーを暗号化するとともに、前記安全なリンクを通じて前記リンクメッセージの１つを介して暗号化された前記コンテンツキーをユーザ機器に伝送するリンク生成ステップと、を含み、
前記リンクメッセージのうち第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つを含み、第２リンクメッセージは、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含むことを特徴とする方法。
【請求項７】
前記ｃ）リンク生成ステップは、
前記ユーザ機器からのリンク要請メッセージをカウントすることによって現在リンク数を生成するステップと、
現在リンク数を最大リンク数と比較することによって、前記現在リンクの回数を制限するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項８】
ｃ）前記リンク生成ステップは、
前記ユーザ機器の公開キーを利用して前記受信装置の個人キーを暗号化した後に、前記ユーザ機器に伝送するステップと、
前記受信装置の公開キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項９】
ｃ）前記リンク生成ステップは、
前記ユーザ機器の公開キーを利用して前記受信装置の秘密キーを暗号化した後に、前記ユーザ機器に伝送するステップと、
前記受信装置の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項１０】
ｃ）前記リンク生成ステップは、
前記受信装置の公開キーを利用して暗号化された前記ユーザ機器の秘密キーを受信するステップと、
前記受信されたユーザ機器の秘密キーを利用して前記コンテンツキーを暗号化した後に、前記ユーザ機器に伝送するステップと、を含むことを特徴とする請求項６に記載の方法。
【請求項１１】
ａ）コンテンツ提供者から放送チャンネルを通じて受信された放送ストリームに基づいてコンテンツを生成するステップと、
ｂ）所定のコンテンツキーを利用して前記コンテンツを暗号化するコンテンツ暗号化ステップと、
ｃ）前記コンテンツ提供者と連結されていない状態でも、ユーザ機器と放送受信装置との間でリンクメッセージを交換することによって、前記ユーザ機器と前記放送受信装置との間の安全なリンクを生成し、前記コンテンツキーを暗号化するとともに、前記安全なリンクを通じて前記リンクメッセージの１つを介して暗号化された前記コンテンツキーをユーザ機器に伝送するリンク生成ステップと、を含み、

前記リンクメッセージのうち第１リンクメッセージは、前記ユーザ機器の公開キー及び前記放送受信装置の公開キーのうち一つと、前記放送受信装置の個人キー、秘密キー及び前記ユーザ機器の秘密キーのうち一つを含むことを特徴とする放送コンテンツを受信する方法をコンピュータで実行させるためのプログラムを記録したコンピュータで読み取り可能な記録媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/003766

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01)i

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)

IPC8 : H04L

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

KR, JP : As above

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/0059939 A1 (Sun Microsystems, Inc.) 25 March 2004 (see abstract, figure 35, claim 1)	1 ~ 11
A	US 2004/0133908 A1 (BroadQ, LLC.) 8 July 2004 (see abstract, figure 1, claim 1)	1 ~ 11
A	US 6636968 B1 (Koninklijke Philips Electronics) 21 October 2003 (see abstract, figure 2, claim 1)	1 ~ 11

☐ Further documents are listed in the continuation of Box C.

☒ 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 application or patent 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 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
03 MARCH 2006 (03.03.2006)	**03 MARCH 2006 (03.03.2006)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	LEE, Dong Hwan Telephone No. 82-42-481-5755

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2005/003766

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US20040059939A1	25.03.2004	US2004059939A1	25.03.2004
		US2004059939AA	25.03.2004
US20040133908A1	08.07.2004	US2004133908A1	08.07.2004
		US2004133908AA	08.07.2004
US6636968B1	21.10.2003	CN1157021C	07.07.2004
		CN1304604	18.07.2001
		CN1304604A	18.07.2001
		CN1304604T	. .T
		EP01080558A1	07.03.2001
		EP1080558A1	07.03.2001
		JP14540721	26.11.2002
		JP2002540721T2	26.11.2002
		KR1020010043748	25.05.2001
		TW543312B	21.07.2003
		US6636968BA	21.10.2003
		WO0059154A1	05.10.2000
		WO200059154A1	05.10.2000

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,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KZ,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,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 スン－ヒュ・ハン
大韓民国・ソウル・ソンパ－グ・ムンジュン・２－ドン・（番地なし）・ファミリー・１－ダンジ・アパート・１０２－１００６
(72)発明者 ミュン－スン・キム
大韓民国・ギョンギ－ド・ウイワン－シ・サム－ドン・（番地なし）・デウー・アパート・１０５－１０４
(72)発明者 ヨン－クック・ユー
大韓民国・ソウル・ソンドン－グ・グンホ－ドン・３－ガ・（番地なし）・ドゥーサン・アパート・１１５－２０６
(72)発明者 ヨン－スン・ヨーン
大韓民国・ギョンギ－ド・スウォン－シ・グウォンソン－グ・グウォンソン－ドン・（番地なし）・サンロク・アパート・５１１－７０４
(72)発明者 ボン－ソン・キム
大韓民国・ギョンギ－ド・ソンナン－シ・ブンダン－グ・グンゴク－ドン・（番地なし）・チョンソル・マウル・ジュゴン・９－ダンジ・アパート・９０３－４１１
(72)発明者 ジェ－フン・イ
大韓民国・ギョンギ－ド・スウォン－シ・ヨントン－グ・メタン・３－ドン・１２５０－８・（２０６）

Ｆターム(参考) 5C164 FA04 PA22 PA25 PA26 UA51S UB03S UB10P UB38S UB41S UB73P
UC22P UC26S YA05 YA16
5J104 AA16 BA03 EA01 EA04 EA15 EA16 EA17 EA19 JA03 JA21
MA05 NA02 NA37 PA05