

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成20年12月25日(2008.12.25)

【公表番号】特表2008-521275(P2008-521275A)

【公表日】平成20年6月19日(2008.6.19)

【年通号数】公開・登録公報2008-024

【出願番号】特願2007-541095(P2007-541095)

【国際特許分類】

H 04 L 9/08 (2006.01)

H 04 N 7/173 (2006.01)

H 04 N 7/167 (2006.01)

【F I】

H 04 L 9/00 6 0 1 B

H 04 N 7/173 6 3 0

H 04 N 7/167 Z

H 04 L 9/00 6 0 1 E

【手続補正書】

【提出日】平成20年11月5日(2008.11.5)

【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) 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するとともに、前記リンクメッセージの1つを介し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、を備える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) 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) 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。