(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2004-506353
(P2004-506353A)
(43)公表日　平成16年2月26日(2004.2.26)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601B	5C063
H04N	7/08	H04N	7/16	Z	5C064
H04N	7/081	H04N	7/08	Z	5J104
H04N	7/16	H04L	9/00	601E	

審査請求 未請求　予備審査請求 有　（全 44 頁）

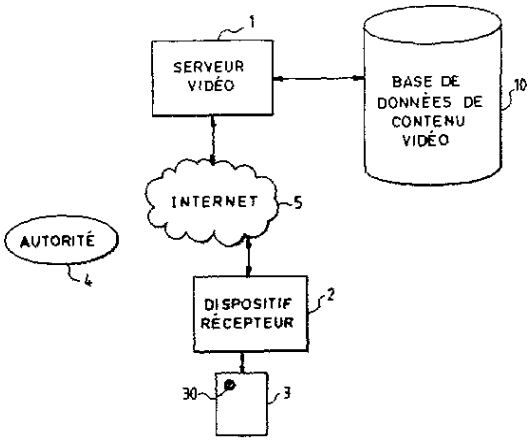
(21)出願番号　特願2002-518080(P2002-518080)
(86)(22)出願日　平成13年7月31日(2001.7.31)
(85)翻訳文提出日　平成15年1月30日(2003.1.30)
(86)国際出願番号　PCT/FR2001/002502
(87)国際公開番号　WO2002/013529
(87)国際公開日　平成14年2月14日(2002.2.14)
(31)優先権主張番号　00/10339
(32)優先日　平成12年8月4日(2000.8.4)
(33)優先権主張国　フランス(FR)

(71)出願人　501263810
トムソン　ライセンシング　ソシエテ　アノニム
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ｓ．Ａ．
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
(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

最終頁に続く

(54)【発明の名称】マルチメディアコンテンツを表すデジタルデータの安全な配信方法

(57)【要約】
本発明は、コンテンツプロバイダによって、デジタルデータを制御語によりスクランブルされた形式でデータベース（１０）内に格納することを可能にする方法に関する。ユーザが配信ネットワーク（５）を介してデータを受信することを希望する場合、ユーザは、コンテンツプロバイダに暗号化鍵を送信する。コンテンツプロバイダは、この暗号化鍵を用いて制御語を暗号化し、それをスクランブルされたデジタルデータと共に、ユーザの受信装置（２）に送信する。受信装置は、制御語を復号化し、デジタルデータをデスクランブルすることができる。



【特許請求の範囲】
【請求項１】
ブロードキャスティングネットワークを介して、コンテンツプロバイダにより、マルチメディアコンテンツを表し、制御語によりスクランブルされたデジタルデータを安全に配信する方法であって、
（ａ）上記ブロードキャスティングネットワークに接続されるコンテンツ受信装置から受信する暗号化鍵を用いて、上記制御語を暗号化する段階と、
（ｂ）上記コンテンツ受信装置に、上記スクランブルされたデジタルデータと、上記コンテンツ受信装置の上記暗号化鍵を用いて暗号化された上記制御語とを送信する段階とを含むことを特徴とする方法。
【請求項２】
上記暗号化鍵は、上記コンテンツ受信装置に関連付けられる一意の公開鍵であることを特徴とする請求項１記載の方法。
【請求項３】
上記段階（ａ）及び上記段階（ｂ）の前に、
上記コンテンツ受信装置の上記公開鍵と上記公開鍵に関連付けられる暗号証明書とを受信する段階と、
上記関連付けられる暗号証明書を解析することにより上記公開鍵の有効性を確認する段階とを含み、
上記段階（ａ）は、上記公開鍵の有効性が確認された場合にのみ行われることを特徴とする請求項２記載の方法。
【請求項４】
上記段階（ａ）及び上記段階（ｂ）の前に、
上記制御語で上記デジタルデータをスクランブルする段階と、
上記コンテンツプロバイダに関連付けられるデータベースに、上記スクランブルされたデジタルデータと、上記デジタルデータをスクランブルするのに使用した上記制御語を格納する段階とを含むことを特徴とする請求項１乃至３のうちいずれか一項記載の方法。
【請求項５】
上記制御語は、制御メッセージ（ＥＣＭ）の中に入れられることによって上記データベース内に格納され、
上記段階（ａ）において、上記制御メッセージは、上記コンテンツ受信装置から受信する上記暗号化鍵を用いて暗号化され、
上記段階（ｂ）において、上記暗号化された制御メッセージは、上記コンテンツ受信装置に送信されることを特徴とする請求項４記載の方法。
【請求項６】
ブロードキャスティングネットワークを介してコンテンツ受信装置に、マルチメディアコンテンツを表し、制御語によりスクランブルされたデジタルデータを安全に配信する方法であって、
上記ブロードキャスティングネットワークに接続される上記コンテンツ受信装置において、
（ｉ）上記コンテンツ受信装置に関連付けられる暗号化鍵をコンテンツプロバイダに送信する段階と、
（ｊ）上記コンテンツプロバイダから、上記スクランブルされたデジタルデータと、上記暗号化鍵を用いて暗号化された上記制御語とを受信する段階と、
（ｋ）上記コンテンツ受信装置の上記暗号化鍵に関連付けられる復号化鍵を用いて、受信した上記制御語を復号化する段階と、
（ｌ）上記デジタルデータをユーザに提示可能な信号に変換するよう、上記復号化された制御語を用いて上記デジタルデータをデスクランブルする段階とを含むことを特徴とする方法。
【請求項７】

上記暗号化鍵は一意の公開鍵であり、上記復号化鍵は、上記公開鍵に関連付けられる一意の秘密鍵であることを特徴とする請求項６記載の方法。
【請求項８】
上記コンテンツ受信装置は、セキュリティ素子と協働可能であり、
上記公開鍵及び上記秘密鍵の対は、上記セキュリティ素子と一意の方法で関連付けられて上記セキュリティ素子内に格納されることを特徴とする請求項７記載の方法。
【請求項９】
上記セキュリティ素子は、信頼できる局によって上記コンテンツ受信装置の上記ユーザに与えられ、
上記セキュリティ素子は、一意の公開鍵及び秘密鍵の対に加えて、上記信頼できる局によって与えられる暗号証明書を含み、
上記段階（ｉ）において、上記コンテンツ受信装置は、上記公開鍵に加えて、上記関連付けられる暗号証明書を上記コンテンツプロバイダに送信することを特徴とする請求項８記載の方法。
【請求項１０】
上記セキュリティ素子は、着脱可能な素子、特に、スマートカードであることを特徴とする請求項８又は９記載の方法。
【請求項１１】
一方でブロードキャスティングネットワーク、特に、インターネットに接続され、他方でデジタルホームネットワークに接続するよう適応されたコンテンツ受信装置に、マルチメディアを表し制御語によりスクランブルされたデジタルデータを安全に配信する方法であって、
上記コンテンツ受信装置において、
（Ａ）上記デジタルホームネットワークに関連付けられる公開鍵を、ブロードキャスティングネットワークを介してコンテンツプロバイダに送信する段階と、
（Ｂ）上記コンテンツプロバイダから、上記ブロードキャスティングネットワークを介して、上記スクランブルされたデジタルデータと上記デジタルホームネットワークの上記公開鍵を用いて暗号化された制御語とを受信する段階と、
（Ｃ）上記スクランブルされたデジタルデータと上記暗号化された制御語を、上記デジタルホームネットワークを介して、上記デジタルホームネットワークに接続される表示装置に送信する段階とを含み、
上記表示装置は、上記デジタルホームネットワークの上記公開鍵に関連付けられる秘密鍵を用いて上記制御語を復号化し、上記デジタルデータをユーザに対し提示可能な信号に変換するよう上記復号化された制御語を用いて上記デジタルデータをデスクランブルすることができることを特徴とする方法。
【請求項１２】
上記コンテンツ受信装置は、第１のセキュリティ素子と協働可能であり、
上記デジタルホームネットワークに関連付けられる上記公開鍵は、上記第１のセキュリティ素子に格納されることを特徴とする請求項１１記載の方法。
【請求項１３】
上記表示装置は第２のセキュリティ素子と協働可能であり、
上記デジタルホームネットワークに関連付けられる上記秘密鍵は、上記第２のセキュリティ素子に格納されることを特徴とする請求項１１又は１２記載の方法。
【請求項１４】
上記第１のセキュリティ素子及び／又は上記第２のセキュリティ素子は、着脱可能な素子、特に、スマートカードであることを特徴とする請求項１２又は１３記載の方法。
【発明の詳細な説明】
【０００１】
［発明の属する技術分野］
本発明は一般的に、ブロードキャスティングネットワーク、特に、インターネットを介し

てデータを配信する方法に係る。より詳細には、本発明は、ビデオ又はオーディオシーケンスといったマルチメディアコンテンツを表すデジタルデータを安全に配信する方法に係る。

【０００２】

［発明の背景］

特にインターネットを介してデジタルデータを安全な方法で配信するための現行のソリューションは、コンテンツプロバイダによって送信されるデータの暗号化と、インターネットに接続されるコンピュータ上で実行され、送信されたデータを受信するアプリケーションによる送信されたデータの解読（復号化）に基本的に基づいている。

【０００３】

しかし、このソリューションは十分な安全性を保証しない。何故なら、コンピュータといった装置において復号化鍵（復号化鍵は安全性を確実にするためには秘密にされなくてはならない）を安全確実に格納することはほとんど不可能であるからである。

【０００４】

更に、コンテンツプロバイダにとっての重要な関心事は、マルチメディアコンテンツを表すデジタルデータの違法複製に対する防御である。

【０００５】

［発明の概要］

本発明は、従来技術よりも安全な、マルチメディアコンテンツを表すデジタルデータの配信方法を提案することを目的とする。

【０００６】

本発明は更に、デジタルデータの違法複製を阻止することができる上述したような方法を提案することを目的とする。

【０００７】

従って、本発明は、ブロードキャスティングネットワークを介して、コンテンツプロバイダにより、マルチメディアコンテンツを表し制御語によりスクランブルされたデジタルデータを安全に配信する方法に係る。

【０００８】

本発明の方法は、

（ａ）ブロードキャスティングネットワークに接続されるコンテンツ受信装置から受信する暗号化鍵を用いて、制御語を暗号化する段階と、

（ｂ）コンテンツ受信装置に、スクランブルされたデジタルデータと、コンテンツ受信装置の暗号化鍵を用いて暗号化された制御語とを送信する段階とを含む。

【０００９】

本発明の有利な実施例では、暗号化鍵は、コンテンツ受信装置に関連付けられる一意の公開鍵である。

【００１０】

対称暗号システムにおいて使用される公開鍵は、公開鍵に関連付けられる秘密鍵によってのみ、公開鍵で暗号化された制御語を復号化することができるので、安全性に特に配慮がされているわけではないネットワークを介して送信することができる。従って、受信装置の公開鍵を送信するのに安全性に配慮のなされたチャネルを用意する必要はない。

【００１１】

本発明の特定の特徴によると、上述した本発明の方法は、段階（ａ）及び（ｂ）の前に、受信装置の公開鍵と、その公開鍵に関連付けられる暗号証明書とを受信する段階と、関連付けられる暗号証明書を解析することにより公開鍵の有効性を確認する段階とを含む。段階（ａ）は有効性が確認された場合にのみ行われる。

【００１２】

本発明のもう１つの有利な実施例によると、上述した本発明の方法は、段階（ａ）及び（ｂ）の前に、制御語でデジタルデータをスクランブルする段階と、コンテンツプロバイダに関連付けられるデータベースに、スクランブルされたデジタルデータと、デジタルデー

タをスクランブルするのに使用した制御語を格納する段階とを含む。
【００１３】
従って、コンテンツプロバイダは、コンテンツ受信装置によるデジタルデータの送信要求を受信する前にデジタルデータをスクランブルする前処理を行う。デジタルデータ送信要求が、コンテンツプロバイダによって受信されると、コンテンツプロバイダは、要求を出した受信装置から受信される鍵を用いて制御語の暗号化を直ぐに行わなければならない。この暗号化演算は、ブロードキャスティングネットワークを介して受信装置にスクランブルされたデジタルデータをダウンロードする瞬間においてリアルタイムに行うことができ、それにより、要求の高速処理が可能となる。
【００１４】
本発明の特定の特徴によると、制御語は、制御メッセージの中に入れられることによってコンテンツプロバイダに関連付けられるデータベース内に格納され、段階（ａ）において、制御メッセージは、コンテンツ受信装置から受信される暗号化鍵を用いて暗号化され、段階（ｂ）において、暗号化された制御メッセージはコンテンツ受信装置に送信される。
【００１５】
本発明の第２の面によると、本発明は更に、ブロードキャスティングネットワークを介してコンテンツ受信装置に、マルチメディアコンテンツを表し、制御語によってスクランブルされたデジタルデータを安全に配信する方法に係る。本発明では、ブロードキャスティングネットワークに接続されるコンテンツ受信装置において以下の方法を含む。
（ｉ）コンテンツ受信装置に関連付けられる暗号化鍵をコンテンツプロバイダに送信する段階と、
（ｊ）コンテンツプロバイダから、スクランブルされたデジタルデータと、暗号化鍵を用いて暗号化された制御語とを受信する段階と、
（ｋ）コンテンツ受信装置の暗号化鍵に関連付けられる復号化鍵を用いて、受信した制御語を復号化する段階と、
（ｌ）デジタルデータをユーザに提示可能な信号に変換するよう、復号化された制御語を用いてデジタルデータをデスクランブルする段階とを含む。
【００１６】
本発明の有利な実施例では、暗号化鍵は一意の公開鍵であり、復号化鍵は、公開鍵に関連付けられる一意の秘密鍵である。
【００１７】
本発明の特定の特徴によると、コンテンツ受信装置は、セキュリティ素子と協働可能であり、公開鍵及び秘密鍵はセキュリティ素子と一意の方法で関連付けられ、セキュリティ素子内に格納される。
【００１８】
本発明の別の特徴によると、セキュリティ素子は、信頼できる局によってコンテンツ受信装置のユーザに与えられる。セキュリティ素子は、一意の公開鍵及び秘密鍵の対に加えて、信頼できる局によって与えられる暗号証明書を含み、また、段階（ｉ）において、コンテンツ受信装置は、公開鍵に加えて、関連付けられる暗号証明書をコンテンツプロバイダに送信する。
【００１９】
本発明の有利な特徴によると、セキュリティ素子は着脱可能な素子、特に、スマートカードである。
【００２０】
本発明の第３の面によると、本発明は更に、コンテンツ受信装置に、マルチメディアコンテンツを表し制御語によってスクランブルされたデジタルデータを安全に配信する方法に係り、コンテンツ受信装置は、一方でブロードキャスティングネットワーク、特にインターネットに接続され、他方でデジタルホームネットワークに接続するよう適応される。本発明の第３の面によると、本発明は、受信装置において以下の段階を含む。
（Ａ）デジタルホームネットワークに関連付けられる公開鍵を、ブロードキャスティング

ネットワークを介して、コンテンツプロバイダに送信する段階と、
（Ｂ）コンテンツプロバイダから、ブロードキャスティングネットワークを介して、スクランブルされたデジタルデータとデジタルホームネットワークの公開鍵を用いて暗号化された制御語とを受信する段階と、
（Ｃ）スクランブルされたデジタルデータと暗号化された制御語を、デジタルホームネットワークを介して、デジタルホームネットワークに接続される表示装置に送信する段階とを含み、表示装置は、デジタルホームネットワークの公開鍵に関連付けられる秘密鍵を用いて制御語を復号化し、デジタルデータをユーザに対し提示可能な信号に変換するよう復号化された制御語を用いてデジタルデータをデスクランブルすることができる。

【００２１】

本発明の有利な実施例によると、コンテンツ受信装置は、第１のセキュリティ素子と協働可能であり、デジタルホームネットワークに関連付けられる公開鍵は第１のセキュリティ素子に格納される。

【００２２】

この実施例では、表示装置は第２のセキュリティ素子と協働可能であり、デジタルホームネットワークに関連付けられる秘密鍵は、第２のセキュリティ素子に格納される。

【００２３】

本発明の有利な特徴によると、第１のセキュリティ素子及び／又は第２のセキュリティ素子は着脱可能な素子、特に、スマートカードである。

【００２４】

［発明の実施様態の詳細な説明］

本発明は、添付図面を参照しながら、特に非制限的な実施例の以下の説明を読むことによりより良好に理解できるであろう。

【００２５】

以下の説明において、ビデオコンテンツであるデジタルデータのみを参照するが、当然ではあるが、本発明は、任意の種類のマルチメディアコンテンツ、例えば、オーディオ、ビデオ、又は、テキストデータのシーケンス、或いは、ソフトウェアを実行するのに使用されるコンピュータデータファイルの配信にも適用される。

【００２６】

図１に、ビデオコンテンツデータベース１０に接続されるビデオサーバ１を示す。データベース１０及びビデオサーバ１は、インターネット５といったブロードキャスティングネットワークを介してビデオコンテンツをユーザに供給するコンテンツプロバイダに属するものである。

【００２７】

ビデオコンテンツを表すデジタルデータは、圧縮され（従って、ブロードキャスティングネットワークによって容易に送信することができる）、且つ、一般的にＣＷと表される制御語によってスクランブルされた形式でデータベース内に格納される。スクランブリングは、鍵と、定期的に更新され、共通情報（ＥＣＭ）と呼ばれる制御メッセージ内に格納される制御語とを用いて対称暗号スキームに応じて行われる。この制御メッセージは、スクランブルされたデータと共にデータベース内に格納される。

【００２８】

デジタルデータをデータベース１０に格納するために、デジタルデータを圧縮及びスクランブルする前処理は、ユーザにデジタルデータを供給する前に行われることが好適である。前処理は、データベース又はビデオサーバ以外で行われてもよい。

【００２９】

デジタルデータのスクランブリングは、ＤＶＢ　ＣＳ（デジタル・ビデオ・ブロードキャスティング・コンテンツ・スクランブリング）規格に則して行われることが好適であり、好適な実施例では、デジタルデータは、ブロードキャスティングネットワークを介して送信されるようＭＰＥＧ２規格（ＩＳＯ／ＩＥＣ　１３８１８‐１）に則して、パケットの形式で符号化される。

【００３０】
図２ａには、データベース１０に格納されるようなデータパケット６のコンテンツを示す。このデータパケットは、スクランブルされたビデオデータ６２と、ビデオデータ６２をスクランブルするのに用いた制御語ＣＷを含むＥＣＭ制御メッセージ６１とを含む。当然ではあるが、ビデオシーケンス全体は、図２ａに示すようなタイプのパケット６が連続する形で、データベース内に格納される。更に、一般的に、デジタルデータをスクランブルするために使用した制御語ＣＷを含むＥＣＭメッセージは、その制御語を使用してスクランブルされたデジタルデータに対し、データストリーム中、先に送信される。
【００３１】
図１を再び参照するに、ビデオサーバ１は、インターネット５にメッセージ又はデータを送信する、又は、インターネット５からメッセージ又はデータを受信する手段を含む。ビデオサーバ１は更に、以下に説明するように、ネットワークを介して送信する前にＥＣＭメッセージを暗号化する手段を含む。
【００３２】
受信装置２もインターネットに接続される。受信装置は一般的に、インターネットを介してビデオプログラムにアクセスしたいユーザ方に置かれる。受信装置２は、具体的には、コンピュータ又はデジタルデコーダ（又は「セットトップボックス」）であってよい。デジタルデコーダは、（キーパッド式、スクリーン式、遠隔制御式等の）ユーザインタフェースを有し、それにより、ユーザが受信したいビデオプログラムを選択することが可能となる。
【００３３】
受信装置も、データストリームがロードされると同時にコンテンツを見ることができるストリーミングによって、又は、コンテンツをリアルタイムで見なくてよいダウンロードによって、インターネットからデータストリームを受信する手段を含む。
【００３４】
受信装置は更に、以下に説明するように、デジタルデータをスクランブルするのに使用した制御語を用いて、受信したスクランブルされたデジタルデータパケットをデスクランブルすることが可能なデスクランブラを含む。
【００３５】
受信装置２は更に、スマートカード３を受け取るスマートカード読取り器を含む。スマートカード３は、当業者にはよく知られているように、暗号鍵といったデータを安全な方法で格納可能にするセキュアプロセッサ３０を含む。
【００３６】
スマートカード３は、コンテンツプロバイダとは関係があっても関係がなくてもよい信用できる局（ｔｒｕｓｔｅｄ ａｕｔｈｏｒｉｔｙ）４により与えられることが好適である。コンテンツプロバイダによってビデオシーケンスが配信されるサービスにアクセスすることができるようにするには、ユーザは最初に、コンテンツプロバイダによって指定される信頼できる局を介してこのサービスに申し込まなければならない（支払いのため、又は、コンテンツプロバイダの取引政策に応じて）。
【００３７】
サービスに申し込むと、ユーザは、一意の秘密鍵K_{Pri_Rec}及び公開鍵K_{Pub_Rec}の対を含むスマートカード３を受け取る。この鍵の対は、スマートカード３に固有である。即ち、信頼できる局から与えられるスマートカードはそれぞれ、同じ局から与えられる他のスマートカードとは異なる秘密／公開鍵の対を含む。鍵の対は信頼できる局４から生成され、更に、局は、公開鍵に関連して、暗号証明書を与える。
【００３８】
このような証明書には、公開鍵が所与のユーザに属するものであり、その証明書はその信頼できる局により署名されたものであることを証明する１組のデータ（例えば、公開鍵、ユーザの識別情報、公開鍵の有効期日）が含まれる。Ｘ５０９（ＩＳＯ／ＩＥＣ ９５９４－８）規格を用いて証明書を生成することが好適である。

【００３９】
例えば、証明書は、以下のような形式を有する。
K_{Pub_Rec}｜ｕｓｅｒ ｎａｍｅ｜ｅｘｐｉｒｙ ｄａｔｅK_{Pub_Rec}｜ｓｉｇｎａｔｕｒｅ
署名は、以下の通りに計算される。
【数１】

$$E_{K_{Pri\_Authority}}(Hash(K_{Pub\_Rec}|User\ name|expiry\ date\ K_{Pub\_Rec}))$$

ただし、「｜」は連接演算を表し、「Ｈａｓｈ（ｘ）」はハッシュ関数を表す。ハッシュ関数とは即ち、１組の入力データ「ｘ」を、一般的には入力データのサイズより小さい固定サイズを有し、入力データを表す１組のデータ「ｙ」に変換する数学関数である。この関数は一方向関数でもあり、即ち、「ｙ」を知りながら、ｙ＝Ｈａｓｈ（ｘ）のように「ｘ」を求めることは不可能である。更に、E_K（Ｍ）は、鍵Ｋを用いてメッセージＭを暗号化する演算を表す。
【００４０】
スマートカード３は更に、金融仲介機関又はコンテンツプロバイダと直接的に支払いプロトコルを設定する手段を含む。マイクロペイメント式、即ち、小額支払い専用の支払いプロトコル、又は、マクロペイメント式、即ち、より多額の支払い専用の支払いプロトコルは、当業者には周知であるのでここでは説明しない。
【００４１】
スマートカード３は更に、以下から明らかとなるように秘密鍵K_{Pri_Prec}を用いて、受け取ったＥＣＭメッセージを復号化する手段を含む。
【００４２】
一般的には、本発明の原理は以下の通りである。ユーザが、自分の受信装置２上でビデオサーバ１から受信したいビデオシーケンスを選択すると、受信装置は、インターネットを介して、共にスマートカード３内に格納される公開鍵K_{Pub_Rec}とその暗号証明書を送信する。次に、ビデオサーバは、暗号証明書を解析することにより公開鍵の有効性を確認し、公開鍵が有効である場合には、ビデオサーバは、受信した公開鍵K_{Pub_Rec}を用いて、対応するビデオデータシーケンスをスクランブルするのに使用した制御語を含むＥＣＭメッセージを暗号化する。つまり、図２ａに示すようなデータパケット６のそれぞれに対し、平文のＥＣＭメッセージ６１は、パケット６のスクランブルデータ６２と同じスクランブルデータ７２を含む図２ｂに示すデータパケット７を形成するよう暗号化されたメッセージ
【外１】

$$E_{K_{Pub\_Rec}}(ECM)$$

に置き換えられる。
【００４３】
要求されたビデオデータのスクランブルされたシーケンスと暗号化されたＥＣＭメッセージを含むデータパケット７は、ビデオサーバによって受信装置に送信される。
【００４４】
受信装置は、このデータを受信すると、そこから暗号化されたＥＣＭメッセージを抽出し、ＥＣＭメッセージをスマートカード３に送る。スマートカード３は、スマートカード３の秘密鍵K_{Pri_Rec}を用いてメッセージを復号化する手段を含む。ビデオデータをスクランブルするのに使用した制御語を含む復号化されたＥＣＭメッセージは、スマート

カードによって受信装置に戻される。
【００４５】
これらの制御語を用いて、且つ、それ自体はよく知られている方法によって受信装置は、要求したビデオシーケンスに対応するデジタルデータをデスクランブルする。
【００４６】
以下に、図３を参照しながら、本発明のマルチメディアコンテンツを表すデータを配信する方法の様々な段階をより詳細に説明する。
【００４７】
図３に示す３本の下方向の垂直軸ｔは、ビデオサーバ１、受信装置２、及び、スマートカード３間のやり取り及びこれらの３つの要素により行われる処理を説明するための時間軸を表す。
【００４８】
第１の段階１００において、ユーザは、受信装置のユーザインタフェースを介してユーザが受信したい、例えば、映画、又は、特定の送信であるビデオシーケンスを選択したものと仮定する。その場合、受信装置２は、ビデオサーバ１のアドレスに対し出されるビデオコンテンツ要求メッセージを構成する。この要求は当然ながら、要求したビデオシーケンスの識別子と受信装置の識別子を含む。
【００４９】
次の段階１０１では、ビデオサーバは、選択されたビデオシーケンスの配信に関する、例えば価格である取引条件を受信装置に送る。取引条件は、ユーザにユーザインタフェースを介して表示され、ユーザは取引を続行するか否かを決定する。
【００５０】
ユーザがやはりビデオシーケンスを受信したい場合、ユーザは、ユーザインタフェースを介して入力されるコマンドによりそのことを示す。段階１０２において、受信装置は、段階１０１において受信した取引条件、又は、取引条件の例えば価格といった特定の要素のみをスマートカード３に送る。
【００５１】
実際には、選択された支払い方法に応じて、スマートカードはビデオシーケンスに対する支払いに関係がない場合もある。例えば、クレジットカードに基づいた支払いプロトコル（例えば、ＳＥＴ（セキュア・エレクトロニック・トランザクション）プロトコルを用いた場合）は関係がない。図３では、スマートカード３は、選択されたビデオシーケンスに対する支払いのために使用されると仮定する（例えば、スマートカードはマイクロペイメントプロトコルを行う「電子財布」機能を含む）。
【００５２】
段階１０３において、スマートカードは以下のものを含むメッセージを受信装置に送る。即ち、
- 支払いに関するデータ
- スマートカード内に格納される一意の公開鍵K_{Pub_Rec}
- この公開鍵に関連付けられる暗号証明書

段階１０４において、このメッセージはそのまま受信装置によってビデオサーバに転送される。スマートカードが支払いに関係しない場合、支払いに関するデータは、受信装置によって、前の段階においてスマートカードから受信したデータに結び付けられ、それにより、段階１０４に送信されるメッセージを形成する。
【００５３】
次に、ビデオサーバは、支払いに関するデータの確認を行う（段階１０５）。これらのデータが、支払いが確実に行われることを証明する場合、ビデオサーバは、公開鍵K_{Pub_Rec}によって受信した暗号証明書を解析することによって公開鍵の有効性を確認する（段階１０６）。
【００５４】
このためには、ビデオサーバは、スマートカード３を供給した信頼できる局４の公開鍵Ｋ

Ｐｕｂ＿Ａｕｔｈｏｒｉｔｙを有する。従って、一方で、
【数２】

$$D_{K_{Pub\_Auhority}}\left(E_{K_{Pri\_Authority}}\left(Hash\left(K_{Pub\_Rec}\middle|User\ name\middle|expiry\ date\ K_{Pub\_Rec}\right)\right)\right)$$

を行うことによって暗号証明書の署名を確認し、ただし、「D_K（Ｍ）」は、鍵Ｋを用いたメッセージＭの復号化演算を表す。他方で、暗号証明書の他のデータを用いて、Ｈａｓｈ（K_{Pub_Rec}｜Ｕｓｅｒ ｎａｍｅ｜ｅｘｐｉｒｙ ｄａｔｅ K_{Pub_Rec}）の演算を行うことができる。

【００５５】
上述した２つの演算は、暗号証明書が改ざんされていない限り、通常は同一の結果をもたらすべきである。

【００５６】
従って、ビデオサーバは、受信装置から受信した公開鍵K_{Pub_Rec}が、確かにスマートカード３を所有するユーザに信頼できる局から割当てられたものであることを確認することができる。

【００５７】
この確認が行われると、次の段階１０７において、ビデオサーバは、公開鍵K_{Pub_Rec}を使用して、ユーザによって選択されたビデオシーケンスに対応するデータをスクランブルするのに使用した制御語を含むＥＣＭメッセージを暗号化する。

【００５８】
ＲＳＡ（発明者であるリヴェスト（Ｒｉｖｅｓｔ）、シャミア（Ｓｈａｍｉｒ）、及び、エイドルマン（Ａｄｌｅｍａｎ）の名前から取られた）暗号アルゴリズムが選択されることが好適であり、この暗号アルゴリズムは、１，０２４ビットの秘密鍵及び公開鍵（信頼できる局４により供給される）を用いるとして当業者によく知られている。

【００５９】
次の段階１０８において、ビデオサーバは暗号化した制御メッセージと、ユーザによって選択されたビデオシーケンスに対応するスクランブルデータとを（前に説明したようにダウンロードすることにより）送信する。

【００６０】
暗号化された制御メッセージは、受信装置において、受信したデータから抽出され、段階１０９において、スマートカード３に転送される。

【００６１】
段階１１０において、スマートカードは、その秘密鍵K_{Pri_Rec}を用いて制御メッセージを復号化し、制御語ＣＷを平文として受信装置に戻す（段階１１１）。

【００６２】
従って、段階１１２において受信装置は、制御語を用いて、段階１０８において受信したデジタルデータをデスクランブルすることができる。これにより、ユーザはこれらのデータを見ることができるようになる（例えば、スクリーンが具備されるコンピュータ上で直接見ることができるようになる）。受信装置は、他の装置にこれらのデータを送信して視聴できるようにしてもよい。

【００６３】
１つの変形として、スマートカード３がデスクランブラを含み、スマートカード内においてデジタルデータのデスクランブリングが行われることも可能である。

【００６４】
以下に、配信されたマルチメディアコンテンツの複製を確実に防御することを可能にする本発明の第２の実施例を説明する。

【００６５】

図１の実施例と共通する構成要素には同一の参照番号が付けられ、従って、ここでは、詳しく説明しない。

【００６６】

図１に示すシステムとの第１の違いは、受信装置２０は、データをダウンロードするのにインターネット５に接続されるのに追加して、デジタルホームネットワーク５０に接続される点である。これ以外は、受信装置２０は、受信装置２と同様の構成要素を含み、特に、信頼できる局４から供給されるスマートカード２１を受け取るカード読取り器を含む。

【００６７】

一方で、スマートカード２１は、信頼できる局により割当てられる公開鍵のみを含む。

【００６８】

前述の公開鍵に関連付けられる秘密鍵を含む第２のスマートカード２５も信頼できる局により供給されるが、第２のスマートカード２５は、デジタルホームネットワーク５０に接続される表示（表現）装置２４のカード読取り器に挿入されるものである。

【００６９】

以下の説明において、スマートカード２１に含まれる公開鍵は、デジタルホームネットワーク５０の公開鍵K_{PUB_DHN}として見なされ、第２のスマートカード２５に含まれる秘密鍵は、デジタルホームネットワーク５０の秘密鍵K_{PRI_DHN}として見なされる。

【００７０】

この第２の実施例の原理は以下に示す通りである。即ち、ユーザがビデオシーケンスを受信したいと望む場合、図３に記載される段階１００乃至１０２が同様に行われる。その後に、デジタルホームネットワークの公開鍵K_{PUB_DHN}（スマートカード２１に格納される）がビデオサーバ１に送信される。ビデオサーバ１は、従って、公開鍵K_{PUB_DHN}を使用してＥＣＭ制御メッセージを暗号化し、選択されたビデオシーケンスに対応するスクランブルデータと共に暗号化されたＥＣＭメッセージを受信装置２０に戻す。

【００７１】

一方で、受信装置に挿入されるスマートカード２１には秘密鍵K_{PRI_DHN}が含まれないので、受信装置２０はデータをデスクランブルすることができない。更に、受信装置２０は任意のデスクランブラを含まないことが好適である。

【００７２】

受信装置２０は、インターネットといった外部のブロードキャスティングネットワークからデータを受信するためのデジタルホームネットワーク用のエントリポイントとしてのみ作用する。

【００７３】

従って、ユーザによって選択されたビデオシーケンスに対応するデジタルデータは、常にスクランブルされた状態でデジタルホームネットワーク５０内の流れることが可能である。これらのデータは、デジタルホームネットワーク５０の秘密鍵K_{PRI_DHN}を含み、デジタルホームネットワーク５０の公開鍵K_{PUB_DHN}によって暗号化されたＥＣＭ制御メッセージを復号化することのできるスマートカード２５を含む表示装置２４（例えば、デジタルテレビジョン）によってのみデスクランブルされることが可能である。

【００７４】

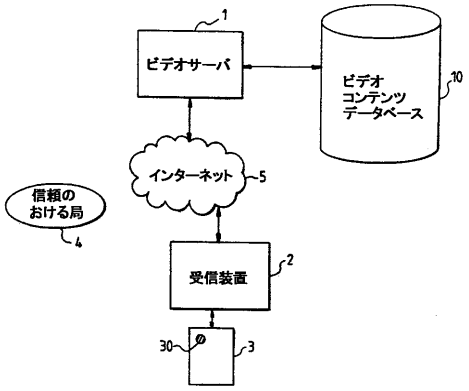
図４には更に、デジタルホームネットワーク５０に接続される記録装置２２が示される。記録装置は特に、デジタルビデオレコーダ、又は、ＤＶＤ（デジタル・バーサトル・ディスク）式の光ディスクに記録可能な機器である。

【００７５】

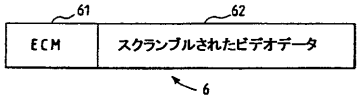
本発明の方法によって、デジタルホームネットワーク５０内を流れるデータはスクランブルされているので、データは、この形式以外で記録装置２２に記録されることはできない。従って、コンテンツプロバイダから受信されるデータのコピーを、インターネット５からダウンロードすることにより作成することはできるが、これらのコピーは、デジタルホームネットワーク５０内においてのみ読取ることができる。

【００７６】
具体的には、スクランブルデータに関連付けられるＥＣＭ制御メッセージは、デジタルホームネットワークの公開鍵K_{PUB_DHN}を用いて暗号化されるので、これらのメッセージは、デジタルホームネットワーク５０に接続される表示装置２４によってのみ復号化することが可能である。
【００７７】
信頼できる局４は、当然のことながら、ユーザに提供される（スマートカード２１、２５の対に含まれる）秘密／公開鍵の対は、全て互いに異なり、一意であることを保証する。従って、デジタルホームネットワーク５０上で作成されたコピーを、別の秘密／公開鍵の対を有する別のデジタルホームネットワーク上で読み出すことは不可能である。
【００７８】
従って、本発明は、コンテンツプロバイダから受信されるデータが違法に複製され、ユーザのホームネットワーク以外で読み出されないことを保証することが可能である。
【００７９】
当然のことながら、デジタルホームネットワーク５０は幾つかの受信装置（それぞれ公開鍵K_{PUB_DHN}を有するスマートカードを含む）、幾つかの表示装置（それぞれ秘密鍵K_{PRI_DHN}を有するスマートカードを含む）、及び、幾つかの記録装置を含むことが可能である。受信装置は、具体的には、デジタルデコーダ又はジュークボックス（インターネットデータをダウンロードすることはできるがそれらを表示することはできない機器）であり、表示（表現）装置は、具体的には、デジタルテレビジョン又はデジタル信号を受信可能なスピーカである。１つの機器が、受信装置と表示装置の機能を同時に満たしてもよく、重要なことは、データは、違法複製を効果的に防御するよう常にスクランブル形式でホームネットワーク内を流れる点である。
【図面の簡単な説明】
【図１】
本発明の第１の実施例の実施を可能にする様々な要素の機能を示す機能ブロック図である。
【図２ａ】
図１に示す要素によりやり取りされるデータを示す図である。
【図２ｂ】
図１に示す要素によりやり取りされるデータを示す図である。
【図３】
本発明の方法を実施する際に、図１の主な要素間で行われるやり取りを示す図である。
【図４】
本発明の第２の実施例示すブロック図である。

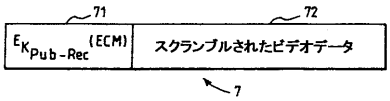
【図１】



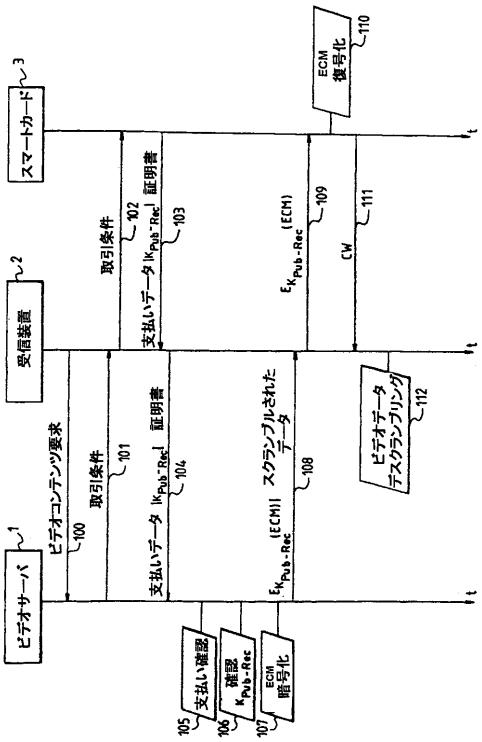
【図２ａ】



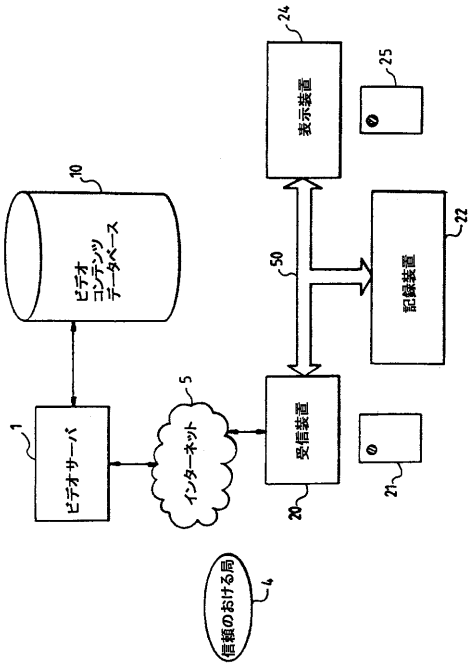
【図２ｂ】



【図３】



【図４】



【国際公開パンフレット】

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 février 2002 (14.02.2002)

PCT

(10) Numéro de publication internationale
WO 02/13529 A1

(51) Classification internationale des brevets[7] : H04N 7/167

(21) Numéro de la demande internationale : PCT/FR01/02502

(22) Date de dépôt international : 31 juillet 2001 (31.07.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/10339 4 août 2000 (04.08.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THOMSON LICENSING SA** [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **DIEHL, Eric** [FR/FR]; La Buzardière, F-35340 Liffre (FR).

(74) Mandataire : **BERTHIER, Karine**; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

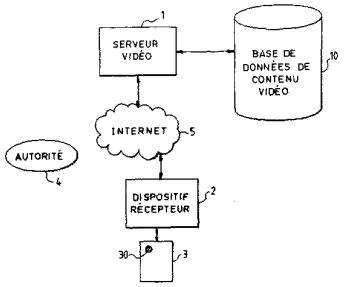
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,

[Suite sur la page suivante]

(54) **Title:** METHOD FOR SECURE DISTRIBUTION OF DIGITAL DATA REPRESENTING A MULTIMEDIA CONTENT

(54) **Titre :** METHODE DE DISTRIBUTION SECURISEE DE DONNEES NUMERIQUES REPRESENTATIVES D'UN CONTENU MULTIMEDIA



1...VIDEO SERVER 2...RECEIVER DEVICE
4...AUTHORITY 10...VIDEO CONTENT DATABASE

(57) **Abstract:** The invention concerns a method whereby the digital data are stored by a content provider in a database (10) in a form scrambled by control words. When a user wishes to receive data through a distribution network (5), he transmits to the content provider an encryption key. The provider encrypts the control words with said key and sends back to the user receiver device (2): the scrambled digital data; and the encrypted control words using said encryption key. The receiver device can then decrypt the control words and descramble the data.

[Suite sur la page suivante]

WO 02/13529 A1

WO 02/13529 A1

MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Les données numériques sont stockées par un fournisseur de contenu dans une base de données (10) sous une forme embrouillée par des mots de contrôle. Lorsqu'un utilisateur désire recevoir des données à travers un réseau de diffusion (5), il transmet au fournisseur de contenu une clé de chiffrement. Le fournisseur chiffre les mots de contrôle avec cette clé et retourne au dispositif de réception (2) de l'utilisateur: les données numériques embrouillées; et le mots de contrôle chiffrés à l'aide de ladite clé de chiffrement. Le dispositif de réception peut alors déchiffrer les mots de contrôle et désembrouiller les données.

Méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia

Domaine de l'invention

La présente invention se rapporte d'une manière générale à la distribution de données à travers des réseaux de diffusion, notamment le réseau Internet. Elle concerne plus particulièrement une méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia, tel que des séquences vidéo ou audio.

Etat de la technique

Les solutions existantes pour distribuer des données numériques de manière sécurisée, par l'intermédiaire du réseau Internet notamment, sont basées essentiellement sur le chiffrement des données transmises par le fournisseur de contenu et le déchiffrement de ces données par une application exécutée sur un ordinateur connecté au réseau et recevant lesdites données.

Cependant, ces solutions ne garantissent pas une sécurité suffisante car il est quasi impossible de stocker de manière sécurisée une clé de déchiffrement (qui doit rester secrète pour garantir la sécurité) dans un appareil tel qu'un ordinateur.

Par ailleurs, une préoccupation importante des fournisseurs de contenu concerne la protection contre la copie des données numériques représentant ces contenus.

Exposé de l'invention

Un but de l'invention est donc de proposer une méthode de distribution de données numériques représentatives d'un contenu multimédia qui soit plus sûre que celles de l'art antérieur.

Un autre but de l'invention est de proposer une telle méthode qui permette en outre d'éviter les copies illicites des données numériques.

L'invention concerne à cet effet une méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia par un fournisseur de contenu à travers un réseau de diffusion, lesdites données étant embrouillées par des mots de contrôle. Selon l'invention, la méthode comprend les étapes consistant à :

(a) chiffrer les mots de contrôle à l'aide d'une clé de chiffrement reçue d'un dispositif de réception de contenu raccordé audit réseau ; et

(b) transmettre audit dispositif de réception de contenu :

- lesdites données numériques embrouillées ; et

- les mots de contrôle chiffrés à l'aide de la clé de chiffrement dudit dispositif de réception de contenu.

Selon un mode de réalisation avantageux de l'invention, la clé de chiffrement est une clé publique unique associée au dispositif de réception de contenu.

Une clé publique, utilisée dans un système cryptographique asymétrique, peut être transmise à travers un réseau non sécurisé puisque seule la clé privée qui lui est associée permet de déchiffrer les mots de contrôle chiffrés avec la clé publique. Ainsi, il n'est pas nécessaire de prévoir un canal sécurisé pour transmettre la clé publique du dispositif de réception.

Selon une caractéristique particulière de l'invention, la méthode précitée comporte les étapes, antérieures aux étapes (a) et (b), consistant à recevoir la clé publique du dispositif de réception et un certificat cryptographique associé à ladite clé publique ; et à vérifier la validité de la clé publique en analysant le certificat cryptographique associé. L'étape (a) n'est effectuée qu'en cas de vérification positive.

Selon un autre mode de réalisation avantageux de l'invention, la méthode précitée comporte les étapes, antérieures aux étapes (a) et (b), consistant à :

embrouiller les données numériques avec les mots de contrôle ;

stocker dans une base de données associée audit fournisseur de contenu :

- les données numériques embrouillées ; et
- les mots de contrôle utilisés pour embrouiller lesdites données.

Ainsi, le fournisseur de contenu effectue le pré-traitement consistant à embrouiller les données numériques avant de recevoir des requêtes de transmission des données par des dispositifs de réception de contenu. Lorsque de telles requêtes sont reçues par le fournisseur de contenu, celui-ci doit juste effectuer le chiffrement des mots de contrôle à l'aide de la clé reçue du dispositif de réception qui a émis la requête. Ce calcul de chiffrement peut être effectué en temps réel au moment du téléchargement des données numériques embrouillées vers le dispositif de réception à travers le réseau de diffusion ce qui permet un traitement rapide de la requête.

Selon une caractéristique particulière de l'invention, les mots de contrôle sont stockés dans la base de données associée au fournisseur de contenu en étant renfermés dans des messages de contrôle et :

- à l'étape (a), les messages de contrôle sont chiffrés à l'aide de la clé de chiffrement reçue du dispositif de réception ; et

- à l'étape (b), les messages de contrôle chiffrés sont transmis au dispositif de réception de contenu.

L'invention concerne également, selon un deuxième aspect, une méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia à un dispositif de réception de contenu à travers un réseau de diffusion, lesdites données numériques étant embrouillées par des mots de contrôle. Selon l'invention, la méthode comprend les étapes consistant pour ledit dispositif de réception de contenu raccordé audit réseau à :

(i) transmettre au fournisseur de contenu une clé de chiffrement associée audit dispositif de réception de contenu ;

(j) recevoir dudit fournisseur de contenu :

- lesdites données numériques embrouillées ; et
- les mots de contrôle chiffrés à l'aide de ladite clé ;

(k) déchiffrer lesdits mots de contrôles reçus à l'aide d'une clé de déchiffrement associée à la clé de chiffrement dudit dispositif de réception ; et

(l) désembrouiller, à l'aide des mots de contrôle déchiffrés, lesdites données numériques pour les transformer en un signal apte à être présenté à un utilisateur.

Selon un mode de réalisation avantageux, la clé de chiffrement est une clé publique unique et la clé de déchiffrement est la clé privée unique associée à ladite clé publique.

Selon une caractéristique particulière de l'invention, le dispositif de réception de contenu est apte à coopérer avec un élément de sécurité, et la paire de clés publique et privée est associée de manière unique audit élément de sécurité et est mémorisée dans ledit élément de sécurité.

Selon une autre caractéristique de l'invention, l'élément de sécurité est fourni à l'utilisateur du dispositif de réception de contenu par une autorité de confiance. L'élément de sécurité contient, en plus de la paire de clés publique et privée unique, un certificat cryptographique délivré par ladite autorité et, à l'étape (i), le dispositif de réception de contenu transmet au fournisseur de contenu, en plus de la clé publique, ledit certificat cryptographique associé.

Selon une caractéristique avantageuse de l'invention, l'élément de sécurité est un élément détachable, notamment une carte à puce.

L'invention concerne également, selon un troisième aspect, une méthode de distribution sécurisée de données numériques représentatives d'un contenu multimedia à un dispositif récepteur de contenu, ledit dispositif étant

adapté à être raccordé d'une part à un réseau de diffusion, notamment le réseau Internet ; et d'autre part à un réseau domestique numérique et lesdites données numériques étant embrouillées par des mots de contrôle. Selon ce troisième aspect de l'invention, la méthode comprend les étapes consistant pour le dispositif de réception à :

(A) transmettre, via le réseau de diffusion, au fournisseur de contenu une clé publique associée audit réseau domestique ;

(B) recevoir, via le réseau de diffusion, dudit fournisseur de contenu :

- lesdites données numériques embrouillées ; et
- les mots de contrôle chiffrés à l'aide de ladite clé publique du réseau domestique ;

(C) transmettre, via le réseau domestique numérique, les données embrouillées et les mots de contrôle chiffrés à un dispositif de présentation raccordé au réseau numérique domestique, ledit dispositif étant apte à :

- déchiffrer les mots de contrôle à l'aide de la clé privée associée à ladite clé publique du réseau domestique ; et
- désembrouiller, à l'aide des mots de contrôle déchiffrés, lesdites données numériques pour les transformer en un signal apte à être présenté à un utilisateur.

Selon un mode de réalisation avantageux, le dispositif de réception de contenu est apte à coopérer avec un premier élément de sécurité, et la clé publique associée au réseau domestique est mémorisée dans ce premier élément de sécurité.

Selon ce mode de réalisation, le dispositif de présentation est apte à coopérer avec un deuxième élément de sécurité, et la clé privée associée au réseau domestique est mémorisée dans ce deuxième élément de sécurité.

Selon une caractéristique avantageuse de l'invention, le premier élément de sécurité et/ou le deuxième élément de sécurité est un élément détachable, notamment une carte à puce.

Brève description des dessins

L'invention sera mieux comprise à la lecture de la description suivante de modes de réalisation particuliers, non limitatifs, de celle-ci faite en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma sous forme de blocs fonctionnels des différents éléments permettant la mise en œuvre d'un premier mode de réalisation de l'invention ;

- les figures 2a et 2b illustrent schématiquement des données qui sont échangées par des éléments de la figure 1 ;

- la figure 3 illustre les échanges intervenant entre les principaux éléments de la figure 1 lors de la mise en œuvre de la méthode de l'invention ;

- la figure 4 est un schéma sous forme de blocs illustrant un deuxième mode de réalisation de l 'invention.

Description détaillée de modes de réalisation de l'invention

Dans la suite de la description, on se réfèrera uniquement à des données numériques représentant un contenu vidéo mais naturellement, l'invention s'applique à la distribution de tout type de contenu multimédia, qu'il s'agisse de séquences de données audio, vidéo ou textuelles ou mêmes de fichiers de données informatiques utilisées pour la mise en œuvre de logiciels.

Sur la figure 1, on a représenté un serveur vidéo 1 relié à une base de données de contenus vidéo 10. Ces éléments sont ceux d'un fournisseur de contenu qui met à la disposition d'utilisateurs des contenus vidéo par l'intermédiaire d'un réseau de diffusion tel que le réseau Internet 5.

Les données numériques représentant les contenus vidéo sont mémorisées dans la base de données sous une forme compressée (de manière à pouvoir être transmises facilement par l'intermédiaire du réseau de diffusion) et embrouillée par des mots de contrôle notés généralement CW (de l'anglais Control Word). Cet embrouillage est effectué selon un schéma cryptographique symétrique avec des clés, les mots de contrôle, qui sont renouvelées périodiquement et qui sont mémorisées dans des messages de contrôle notés ECM (de l'anglais « Entitlement Control Message »). Ces messages de contrôle sont mémorisés, avec les données embrouillées, dans la base de données.

Ce pré-traitement consistant à compresser et embrouiller les données pour les mémoriser dans la base de données 10 est préférentiellement effectué avant de mettre les données à disposition des utilisateurs. Il peut même être effectué en dehors de la base de données ou du serveur vidéo.

L'embrouillage des données est préférentiellement effectué selon la norme DVB CS (de l'anglais « Digital Video Broadcasting Content Scrambling » signifiant littéralement « Diffusion Vidéo Numérique Embouillage du Contenu ») et les données sont, dans un mode de réalisation préférentiel, codées sous forme de paquets selon la norme MPEG 2 (ISO/IEC 13818-1) pour être transmises sur le réseau de diffusion.

On a représenté à la figure 2a, de manière schématisée, le contenu d'un paquet de données 6 tel qu'il est mémorisé dans la base de données 10.

Ce paquet de données comporte des données vidéo embrouillées 62 et un message de contrôle ECM 61 qui contient le mot de contrôle CW utilisé pour embrouiller les données 62. Naturellement, une séquence vidéo complète est mémorisée dans la base de données sous la forme d'une succession de paquets du type du paquet 6 de la figure 2a. On notera également que généralement, les messages ECM contenant les mots de contrôle ayant servi à embrouiller des données numériques sont transmis en avance, dans le flux de données, par rapport aux données embrouillées avec ces mots de contrôle.

En revenant à la figure 1, le serveur vidéo 1 comporte des moyens pour envoyer ou recevoir des messages ou des données vers ou du réseau Internet 5. Il comporte également des moyens pour chiffrer les messages ECM avant de les transmettre sur le réseau comme on le verra ci-dessous.

Un dispositif récepteur 2 est également relié au réseau Internet. Ce dispositif récepteur est généralement disposé chez un utilisateur qui désire accéder à des programmes vidéo par le réseau Internet. Il peut s'agir notamment d'un ordinateur ou d'un décodeur numérique (ou « Set-Top Box » en anglais). Celui-ci possède une interface utilisateur (du type clavier, écran, télécommande, etc.) pour permettre notamment à un utilisateur de sélectionner des programmes vidéo qu'il souhaite recevoir.

Le dispositif récepteur comporte également des moyens pour recevoir des flux de données du réseau Internet, par téléchargement en temps réel (« streaming » an anglais), c'est à dire en visualisant le contenu au fur et à mesure du chargement, ou en différé (« downloading » en anglais) c'est à dire sans visualisation en temps réel du contenu.

Il comporte aussi un désembrouilleur (« descrambler » en anglais) capable de désembrouiller comme on le verra ci-dessous, des paquets de données numériques embrouillées qu'il reçoit, à l'aide des mots de contrôle qui ont servi à embrouiller les données.

Le dispositif récepteur 2 comporte en outre un lecteur de carte à puce destiné à recevoir une carte 3. La carte à puce 3 comporte un processeur sécurisé 30 qui, comme cela est bien connu de l'homme de l'art, permet de mémoriser de manière sécurisée des données telles que des clés cryptographiques.

La carte à puce 3 est délivrée de manière préférentielle par une autorité de confiance 4 qui peut être dépendante ou indépendante du fournisseur de contenu. Pour pouvoir accéder au service de distribution de séquences vidéo par le fournisseur de contenu, un utilisateur doit d'abord s'abonner à ce service auprès de l'autorité de confiance désignée par le

fournisseur de contenu (contre paiement ou non selon la politique commerciale du fournisseur de contenu).

L'utilisateur reçoit en échange une carte à puce 3 qui contient une paire de clés privée K_{Pri_Rec} et publique K_{Pub_Rec} unique propre à la carte 3, c'est à dire que chaque carte à puce fournie par l'autorité de confiance comporte une paire de clés privée/publique différente de celle des autres cartes fournies par la même autorité. La paire de clés est générée par l'autorité de confiance 4 et cette dernière fournit, associé à la clé publique, un certificat cryptographique.

Un tel certificat contient un ensemble de données (telles que la clé publique, l'identification de l'utilisateur, une date de validité de la clé publique) qui attestent que la clé publique appartient bien à une personne donnée et il est signé par l'autorité de confiance. On utilisera préférentiellement le standard X509 (ISO/IEC 9594-8) pour générer le certificat.

Par exemple, le certificat pourra avoir la forme suivante :

K_{Pub_Rec}|Nom utilisateur|date expiration K_{Pub_Rec}|signature

La signature étant calculée comme suit :

$$E_{K_{Pri\_Autorité}}\left(\text{Hash}\left(K_{Pub\_Rec}\,|\,\text{Nom utilisateur}\,|\,\text{date expiration}\;K_{Pub\_Rec}\right)\right)$$

avec :

- « | » représentant l'opération de concaténation ;
- « Hash (x) » représentant une fonction de hachage, c'est à dire une fonction mathématique qui transforme un ensemble de données d'entrée « x » en un ensemble de données « y » de taille fixe, souvent inférieure à la taille des données d'entrée, et représentatives des données d'entrées ; cette fonction étant de plus une fonction à sens unique (« one way function » en anglais) c'est à dire que, connaissant « y », il est impossible de retrouver « x » tel que y= Hash(x) ; et
- $E_K(M)$ représente l'opération de chiffrement du message M avec la clé K.

La carte à puce 3 contient également de manière préférentielle des moyens pour établir un protocole de paiement avec un intermédiaire financier ou directement avec le fournisseur de contenu. Les protocoles de paiement, de type micro-paiement, c'est à dire dédiés à des paiements de faibles montants, ou de type macro-paiement, pour des montants plus élevés, sont biens connus de l'homme du métier et ne seront pas décrit plus avant.

La carte à puce 3 comporte aussi des moyens pour déchiffrer les messages ECM qu'elle reçoit à l'aide de la clé privée K_{Pri_Rec} comme on le verra ci-dessous.

D'une manière générale, le principe de l'invention est le suivant : lorsqu'un utilisateur a sélectionné une séquence vidéo qu'il souhaite recevoir du serveur vidéo 1 sur son dispositif récepteur 2, le dispositif récepteur transmet, via le réseau Internet, la clé publique K_{Pub_Rec} ainsi que son certificat mémorisés dans la carte à puce 3. Le serveur vidéo vérifie alors la validité de la clé publique en analysant le certificat et, si la clé publique est valide, le serveur vidéo chiffre les messages ECM contenant les mots de contrôle ayant servi à embrouiller la séquence de données vidéo correspondante avec la clé publique K_{Pub_Rec} reçue. C'est à dire que, pour chaque paquet de données 6 tel celui de la figure 2a, le message ECM 61 en clair est remplacé par un message chiffré $E_{K_{Pub\_Rec}}(ECM)$ 71 pour former un paquet de données 7 (figure 2b) qui contient les mêmes données embrouillées 72 que celles 62 du paquet 6.

Le serveur vidéo transmet ensuite au dispositif récepteur les paquets de données 7 contenant la séquence demandée de données vidéo embrouillées et les messages ECM chiffrés.

Le dispositif récepteur, lorsqu'il reçoit ces données, en extrait les messages ECM chiffrés et il les transmet à la carte à puce 3 qui comporte des moyens pour déchiffrer lesdits messages à l'aide de la clé privée K_{Pri_Rec} de la carte. La carte renvoie au dispositif récepteur les messages ECM déchiffrés qui contiennent les mots de contrôle ayant servi à embrouiller les données vidéo.

A l'aide de ces mots de contrôle, et de manière bien connue en soit, le dispositif récepteur désembrouille les données numériques correspondant à la séquence vidéo demandée.

Nous allons maintenant décrire de manière plus détaillée, en liaison avec la figure 3, les différentes étapes de la méthode de distribution de données représentatives de contenus multimédias de l'invention.

Sur la figure 3, on a représenté par trois axes verticaux descendants t l'axe du temps pour illustrer les échanges entre le serveur vidéo 1, le dispositif récepteur 2 et la carte à puce 3 ainsi que les traitements effectués par ces trois éléments.

Lors de la première étape 100, on suppose que l'utilisateur a sélectionné, par l'intermédiaire de l'interface utilisateur du dispositif récepteur, une séquence vidéo, par exemple un film ou une émission particulière, qu'il souhaite recevoir. Le dispositif récepteur 2 construit alors un message de requête de contenu vidéo qu'il émet à l'adresse du serveur vidéo 1. Cette

requête contient naturellement un identifiant de la séquence vidéo demandée ainsi qu'un identifiant du dispositif récepteur.

A l'étape suivante 101, le serveur vidéo envoie en retour au dispositif récepteur les conditions commerciales, incluant le prix, relatives à la délivrance de la séquence vidéo choisie. Ces conditions sont présentées à l'utilisateur par l'intermédiaire de l'interface utilisateur et celui-ci décide alors s'il souhaite poursuivre la transaction ou non.

Dans le cas où il souhaite toujours recevoir la séquence vidéo, l'utilisateur le signifie par une commande saisie par l'interface utilisateur et, à l'étape 102, le dispositif récepteur envoie à la carte à puce 3 les conditions commerciales reçues à l'étape 101 ou seulement certains éléments, tels que le prix, de ces conditions.

En fait, selon la méthode de paiement choisie, la carte à puce pourra ne pas être impliquée dans le paiement de la séquence vidéo, par exemple dans le cas où un protocole de paiement basé sur une carte de crédit est utilisé (tel que le protocole SET, de l'anglais « Secure Electronic Transaction »). Nous supposons dans l'exemple de la figure 3 que la carte à puce 3 est utilisée pour le paiement de la séquence vidéo choisie (par exemple la carte à puce comporte une fonction « porte-monnaie électronique » mettant en œuvre un protocole de micro-paiement).

La carte à puce envoie donc, à l'étape 103, à l'attention du dispositif récepteur, un message contenant :

- des données relatives au paiement ;
- la clé publique unique K_{Pub_Rec} mémorisée dans la carte ; et
- le certificat associé à cette clé publique.

Ce message est retransmis tel quel par le dispositif récepteur au serveur vidéo à l'étape 104. Dans le cas où la carte à puce n'est pas impliquée dans le paiement, les données concernant le paiement sont concaténées par le dispositif récepteur aux données reçues de la carte à puce à l'étape précédente pour former le message transmis à l'étape 104.

Le serveur vidéo procède alors à la vérification des données concernant la paiement (étape 105). Si ces données prouvent que le paiement a bien été effectué, alors le serveur vérifie la validité de la clé publique K_{Pub_Rec} en analysant le certificat reçu avec cette clé (étape 106).

Pour cela, le serveur possède la clé publique $K_{Pub\_Autorité}$ de l'autorité de confiance 4 qui délivre les cartes à puces 3. Il peut donc d'une part vérifier la signature du certificat en effectuant l'opération :

$D_{K_{Pub\_Autorité}}\left(E_{K_{Pri\_Autorité}}\left(\text{Hash}\left(K_{Pub\_Rec}\,|\,\text{Nom utilisateur}\,|\,\text{date expiration } K_{Pub\_Rec}\right)\right)\right)$

avec « $D_K(M)$ » représentant l'opération de déchiffrement, avec la clé K, du message M et d'autre part effectuer l'opération :

Hash (K_{Pub_Rec}|Nom utilisateur|date expiration K_{Pub_Rec}) à l'aide des autres données du certificat.

Les deux opération ci-dessus doivent normalement donner le même résultat si le certificat n'a pas été altéré.

Le serveur peut ainsi vérifier que la clé publique K_{Pub_Rec} reçue du dispositif récepteur est bien celle qui a été attribuée par l'autorité de confiance à l'utilisateur qui possède la carte à puce 3.

Une fois cette vérification faite, à l'étape suivante 107, le serveur chiffre, avec la clé K_{Pub_Rec}, les messages ECM contenant les mots de contrôle utilisés pour embrouiller les données correspondant à la séquence vidéo choisie par l'utilisateur.

On choisira de préférence l'algorithme cryptographique RSA (du nom des créateurs Rivest, Shamir et Adleman), bien connu de l'homme du métier en utilisant des clés privées et publiques (délivrées par l'autorité de confiance 4) de taille 1024 bits.

A l'étape suivante 108, le serveur transmet (par téléchargement comme on l'a vu plus haut) les messages de contrôles chiffrés et les données embrouillées correspondant à la séquence choisie par l'utilisateur.

Le dispositif récepteur extrait alors des données reçues les messages de contrôle chiffrés et il les transfère à la carte à puce 3 à l'étape 109.

A l'étape 110, la carte à puce déchiffre les messages de contrôle avec sa clé privée K_{Pri_Rec} et elle retourne les mots de contrôle CW en clair au dispositif récepteur (étape 111).

Celui-ci est alors en mesure, à l'étape 112, de désembrouiller les données numériques reçues à l'étape 108, avec ces mots de contrôle. Il peut ensuite directement présenter ces données à l'utilisateur pour qu'il les visualise (par exemple s'il s'agit d'un ordinateur équipé d'un écran). Mais il peut aussi transmettre ces données à un autre dispositif pour visualisation.

En variante, il est également possible que la carte à puce 3 comporte un désembrouilleur et que le désembrouillage des données numériques soit effectué dans la carte à puce.

Nous allons maintenant décrire un deuxième mode de réalisation de l'invention qui permet en outre d'assurer une protection contre la copie des contenus multimédias distribués.

Les éléments communs avec le mode de réalisation de la figure 1 portent les mêmes numéros de référence et ne seront pas décrits davantage.

La première différence avec le système de la figure 1 est que le dispositif récepteur 20, en plus d'être relié au réseau Internet 5 pour télécharger des données, est raccordé à un réseau domestique numérique 50. A part cela, le dispositif récepteur 20 comporte les mêmes éléments que le dispositif récepteur 2, notamment un lecteur de carte à puce adapté à recevoir une carte 21 délivrée par l'autorité de confiance 4.

En revanche, la carte à puce 21 contient seulement une clé publique attribuée par l'autorité de confiance.

Une deuxième carte à puce 25 contenant la clé privée associée à ladite clé publique est également délivrée à l'utilisateur par l'autorité de confiance mais celle-ci est destinée à être insérée dans le lecteur de carte d'un dispositif de présentation 24, également raccordé au réseau domestique numérique 50.

On considèrera dans la suite de la description que la clé publique contenue dans la carte 21 est la clé publique K_{PUB_DHN} du réseau domestique 50 et que la clé privée contenue dans la carte 25 est la clé privée K_{PRI_DHN} du réseau domestique 50.

Le principe de ce mode de réalisation est le suivant : lorsqu'un utilisateur désire recevoir une séquence vidéo, les étapes 100 à 102 décrites à la figure 3 se déroulent de la même manière à la suite de quoi, la clé publique du réseau domestique K_{PUB_DHN} (mémorisée dans la carte à puce 21) est transmise au serveur vidéo 1. Celui-ci chiffre donc les messages de contrôle ECM avec la clé K_{PUB_DHN} et retourne ces messages chiffrés, avec les données embrouillées correspondant à la séquence vidéo choisie, au dispositif récepteur 20.

Par contre, comme la carte à puce 21 insérée dans ce dernier ne contient pas la clé privée K_{PRI_DHN}, le dispositif récepteur 20 ne peut pas désembrouiller les données. D'ailleurs, d'une manière préférentielle, le dispositif récepteur 20 ne comporte pas de désembrouilleur.

Ce dispositif récepteur sert uniquement de point d'entrée sur le réseau domestique numérique pour recevoir des données d'un réseau de diffusion externe tel qu'Internet.

Les données numériques correspondant à la séquence vidéo choisie par l'utilisateur peuvent donc circuler dans le réseau domestique 50 en étant toujours embrouillées. Elles ne seront désembrouillées que dans un dispositif de présentation 24 (par exemple un téléviseur numérique) qui comporte une carte à puce 25, contenant la clé privée K_{PRI_DHN} du réseau domestique 50, capable de déchiffrer les messages de contrôle ECM chiffrés avec la clé publique K_{PUB_DHN} du réseau domestique.

On a également représenté à la figure 4 un dispositif d'enregistrement 22 raccordé au réseau domestique numérique 50. Ce dispositif est notamment un magnétoscope numérique ou un appareil capable d'enregistrer des disque optiques, du type DVD (de l'anglais « Digital Versatile Disc » signifiant littéralement « Disque polyvalent numérique »).

Grâce à la méthode de l'invention, comme les données qui circulent sur le réseau domestique 50 sont embrouillées, celles-ci ne peuvent être enregistrées que sous cette forme par le dispositif d'enregistrement 22. Il est ainsi possible de réaliser des copies des données reçues du fournisseur de contenu par téléchargement du réseau Internet 5 mais ces copies ne peuvent être relues que dans le réseau domestique 50.

En effet, comme les messages de contrôle ECM associés aux données embrouillées sont chiffrés à l'aide de la clé publique du réseau domestique K_{PUB_DHN}, ces messages ne peuvent être déchiffrés que par le dispositif de présentation 24 raccordé au réseau domestique 50.

L'autorité de confiance 4 s'assure bien entendu que les paires de clés privées/publiques (contenues dans les paires de cartes 21, 25) qu'elle fournit aux utilisateurs sont toutes différentes les unes des autres et sont uniques. Il est donc impossible de relire une copie effectuée sur le réseau domestique 50 sur un autre réseau domestique qui possèdera une autre paire de clés privée/publique.

L'invention permet donc de garantir que les données reçues du fournisseur de contenu ne seront pas copiées de manière illicite pour être relues en dehors du réseau domestique de l'utilisateur.

Naturellement, le réseau domestique 50 peut comporter plusieurs dispositifs récepteurs (qui contiennent une carte à puce contenant la clé publique K_{PUB_DHN}), plusieurs dispositifs de présentation (qui contiennent une carte à puce contenant la clé privée K_{PRI_DHN}) et plusieurs dispositifs d'enregistrement. Les dispositifs récepteurs sont notamment un décodeur numérique ou un juke-box (appareil capable de télécharger des données d'Internet mais pas de les présenter) ; les dispositif de présentation sont

notamment un téléviseur numérique ou des haut-parleurs capables de recevoir un signal numérique. Il est également possible qu'un appareil remplisse à la fois la fonction de récepteur et de dispositif de présentation, l'important étant que les données circulent toujours dans le réseau domestique sous forme embrouillée garantissant une protection efficace contre les copies illicites.

REVENDICATIONS

1. Méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia par un fournisseur de contenu à travers un réseau de diffusion (5), lesdites données étant embrouillées par des mots de contrôle (CW), caractérisée en ce qu'elle comprend les étapes consistant à :

(a) chiffrer (107) les mots de contrôle à l'aide d'une clé de chiffrement (K_{Pub_Rec} ; K_{PUB_DHN}) reçue d'un dispositif de réception de contenu (2, 20) raccordé audit réseau ; et

(b) transmettre (108) audit dispositif de réception de contenu :

- lesdites données numériques embrouillées ; et
- les mots de contrôle chiffrés à l'aide de la clé de chiffrement dudit dispositif de réception de contenu.

2. Méthode selon la revendication 1, caractérisée en ce que la clé de chiffrement (K_{Pub_Rec}) est une clé publique unique associée audit dispositif de réception de contenu.

3. Méthode selon la revendication 2, caractérisée en ce qu'elle comporte les étapes, antérieures aux étapes (a) et (b), consistant à :

recevoir (104) la clé publique (K_{Pub_Rec}) du dispositif de réception et un certificat cryptographique associé à ladite clé publique ; et

vérifier (106) la validité de la clé publique en analysant le certificat cryptographique associé,

l'étape (a) n'étant effectuée qu'en cas de vérification positive.

4. Méthode selon l'une des revendications 1 à 3, caractérisée en ce qu'elle comporte les étapes, antérieures aux étapes (a) et (b), consistant à :

embrouiller les données numériques avec les mots de contrôle ;

stocker dans une base de données (10) associée audit fournisseur de contenu :

- les données numériques embrouillées ; et
- les mots de contrôle (CW) utilisés pour embrouiller lesdites données.

5. Méthode selon la revendication 4, caractérisée en ce que les mots de contrôle sont stockés dans ladite base de données en étant renfermés dans des messages de contrôle (ECM) et en ce que :

- à l'étape (a), lesdits messages de contrôle (ECM) sont chiffrés à l'aide de la clé de chiffrement reçue du dispositif de réception ; et
- à l'étape (b), les messages de contrôle chiffrés sont transmis au dispositif de réception de contenu.

6. Méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia à un dispositif de réception de contenu (2) à travers un réseau de diffusion (5), lesdites données numériques étant embrouillées par des mots de contrôle (CW), caractérisée en ce qu'elle comprend les étapes consistant pour ledit dispositif de réception de contenu raccordé audit réseau à :

(i) transmettre (104) au fournisseur de contenu une clé de chiffrement (K_{Pub_Rec}) associée audit dispositif de réception de contenu ;

(j) recevoir (108) dudit fournisseur de contenu :

- lesdites données numériques embrouillées ; et
- les mots de contrôle chiffrés à l'aide de ladite clé (K_{Pub_Rec}) ;

(k) déchiffrer (110) lesdits mots de contrôles reçus à l'aide d'une clé de déchiffrement (K_{Pri_Rec}) associée à la clé de chiffrement dudit dispositif de réception ; et

(l) désembrouiller (112), à l'aide des mots de contrôle déchiffrés, lesdites données numériques pour les transformer en un signal apte à être présenté à un utilisateur.

7. Méthode selon la revendication 6, caractérisée en ce que la clé de chiffrement est une clé publique unique (K_{Pub_Rec}) et la clé de déchiffrement est la clé privée unique (K_{Pri_Rec}) associée à ladite clé publique.

8. Méthode selon la revendication 7, caractérisée en ce que le dispositif de réception de contenu (2) est apte à coopérer avec un élément de sécurité (3), et

en ce que la paire de clés publique et privée est associée de manière unique audit élément de sécurité et est mémorisée dans ledit élément de sécurité.

9. Méthode selon la revendication 8, caractérisée en ce que l'élément de sécurité (3) est fourni à l'utilisateur du dispositif de réception de contenu (2) par une autorité de confiance (4) ;

en ce que ledit élément de sécurité contient, en plus de la paire de clés publique et privée unique, un certificat cryptographique délivré par ladite autorité et

en ce que, à l'étape (i), le dispositif de réception de contenu (2) transmet au fournisseur de contenu, en plus de la clé publique (K_{Pub_Rec}), ledit certificat cryptographique associé.

10. Méthode selon l'une des revendications 8 ou 9, caractérisée en ce que l'élément de sécurité est un élément détachable, notamment une carte à puce.

11. Méthode de distribution sécurisée de données numériques représentatives d'un contenu multimedia à un dispositif récepteur de contenu (20), ledit dispositif étant adapté à être raccordé

d'une part à un réseau de diffusion (5), notamment le réseau Internet ; et

d'autre part à un réseau domestique numérique (50) ;

et lesdites données numériques étant embrouillées par des mots de contrôle, caractérisée en ce qu'elle comprend les étapes consistant pour le dispositif de réception à :

(A) transmettre, via le réseau de diffusion, au fournisseur de contenu une clé publique (K_{PUB_DHN}) associée audit réseau domestique ;

(B) recevoir, via le réseau de diffusion, dudit fournisseur de contenu :

- lesdites données numériques embrouillées ; et
- les mots de contrôle chiffrés à l'aide de ladite clé publique (K_{PUB_DHN}) du réseau domestique ;

(C) transmettre, via le réseau domestique numérique, les données embrouillées et les mots de contrôle chiffrés à un dispositif de présentation (24) raccordé au réseau numérique domestique, ledit dispositif étant apte à :

- déchiffrer les mots de contrôle à l'aide de la clé privée (K_{PRI_DHN}) associée à ladite clé publique du réseau domestique ; et
- désembrouiller, à l'aide des mots de contrôle déchiffrés, lesdites données numériques pour les transformer en un signal apte à être présenté à un utilisateur.

12. Méthode selon la revendication 11, caractérisée en ce que le dispositif de réception de contenu est apte à coopérer avec un premier élément de sécurité (21), et

en ce que la clé publique (K_{PUB_DHN}) associée au réseau domestique est mémorisée dans ledit premier élément de sécurité.

13. Méthode selon l'une des revendications 11 ou 12, caractérisée en ce que le dispositif de présentation est apte à coopérer avec un deuxième élément de sécurité (25), et

en ce que la clé privée (K_{PRI_DHN}) associée au réseau domestique est mémorisée dans ledit deuxième élément de sécurité.

14. Méthode selon l'une des revendications 12 ou 13, caractérisée en ce que le premier élément de sécurité et/ou le deuxième élément de sécurité est un élément détachable, notamment une carte à puce.

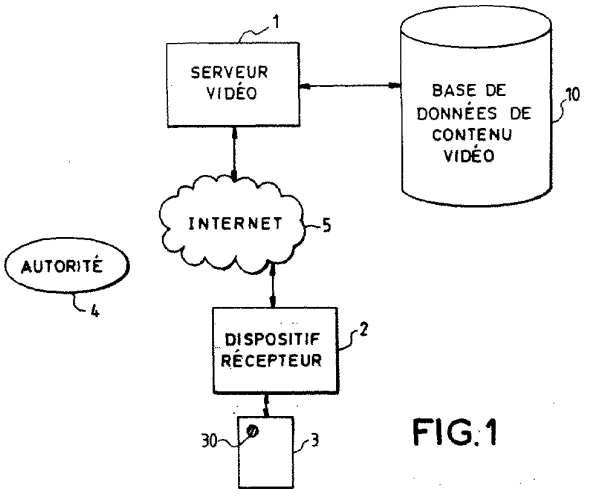


FIG.1

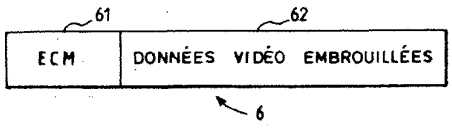


FIG.2a

FIG.2b

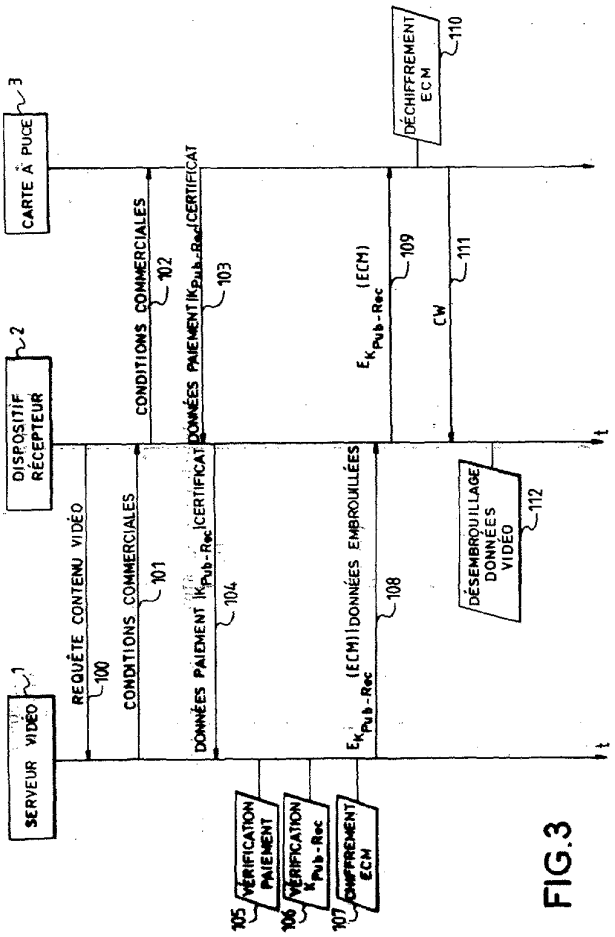

SERVEUR VIDÉO
1
DISPOSITIF RÉCEPTEUR
2
CARTE À PUCE
3
REQUÊTE CONTENU VIDÉO
100
CONDITIONS COMMERCIALES
101
CONDITIONS COMMERCIALES
102
DONNÉES PAIEMENT
CERTIFICAT
103
DONNÉES PAIEMENT
CERTIFICAT
104
VÉRIFICATION PAIEMENT
105
VÉRIFICATION
106
CHIFFREMENT ECM
107
(ECM) DONNÉES EMBROUILLÉES
108
(ECM)
109
CW
111
DÉCHIFFREMENT ECM
110
DÉSEMBROUILLAGE DONNÉES VIDÉO
112
t
t

FIG.3

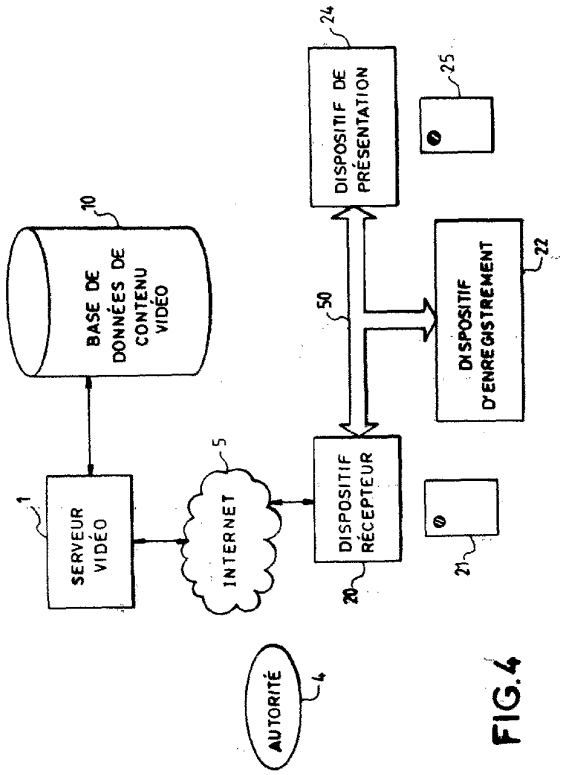

BASE DE DONNÉES DE CONTENU VIDÉO
10
SERVEUR VIDÉO
1
INTERNET
5
DISPOSITIF RÉCEPTEUR
20
DISPOSITIF DE PRÉSENTATION
24
25
DISPOSITIF D'ENREGISTREMENT
22
50
21
AUTORITÉ
4

FIG.4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02502

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167

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

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.
X Y	WO 99 07149 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) the whole document	1,2,6-8, 10 11
Y	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) the whole document	11
A	WO 97 04553 A (PHILIPS ELECTRONICS NV ;PHILIPS NORDEN AB (SE)) 6 February 1997 (1997-02-06) page 1, line 9 - line 16 page 7, line 1 - line 18 figure 1	1-14
A	US 5 563 950 A (MERZ WILLIAM A ET AL) 8 October 1996 (1996-10-08) column 1 -column 2, line 33	1-14

-/--

[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
30 November 2001	06/12/2001

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	Tito Martins, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02502

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 586 022 A (FISCHER ADDISON M) 9 March 1994 (1994-03-09) the whole document	1-14
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW- TECHNICAL,EUROPEAN BROADCASTING UNION. BRUSSELS,BE, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 the whole document	1-14

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/02502

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9907149	A	11-02-1999	AU 1581699	A	08-03-1999
			AU 8670598	A	22-02-1999
			AU 8679798	A	22-02-1999
			AU 8679898	A	22-02-1999
			AU 8764298	A	22-02-1999
			AU 8823398	A	22-02-1999
			AU 8823698	A	22-02-1999
			BR 9810967	A	30-10-2001
			BR 9815607	A	13-11-2001
			EP 1010323	A1	21-06-2000
			EP 1010324	A1	21-06-2000
			EP 1010325	A1	21-06-2000
			EP 1013091	A1	28-06-2000
			EP 1000508	A1	17-05-2000
			EP 1000509	A1	17-05-2000
			EP 1000511	A2	17-05-2000
			JP 2001513587	T	04-09-2001
			JP 2001512842	T	28-08-2001
			WO 9907145	A1	11-02-1999
			WO 9907146	A1	11-02-1999
			WO 9907147	A1	11-02-1999
			WO 9907148	A1	11-02-1999
			WO 9907149	A1	11-02-1999
			WO 9909743	A2	25-02-1999
			WO 9907150	A1	11-02-1999
			US 6105134	A	15-08-2000
			US 6292568	B1	18-09-2001
			US 6252964	B1	26-06-2001
			US 2001001014	A1	10-05-2001
			US 6246767	B1	12-06-2001
EP 0858184	A	12-08-1998	IL 120174	A	28-10-1999
			EP 0858184	A2	12-08-1998
			US 6178242	B1	23-01-2001
			GB 2322030	A ,B	12-08-1998
WO 9704553	A	06-02-1997	EP 0793880	A1	10-09-1997
			WO 9704553	A1	06-02-1997
			JP 10505995	T	09-06-1998
US 5563950	A	08-10-1996	US 5559889	A	24-09-1996
			JP 8278750	A	22-10-1996
EP 0586022	A	09-03-1994	US 5005200	A	02-04-1991
			EP 0586022	A1	09-03-1994
			AT 113429	T	15-11-1994
			AT 150605	T	15-04-1997
			AU 620291	B2	13-02-1992
			AU 4242589	A	13-09-1990
			CA 2000400	A1	07-09-1990
			DE 69013541	D1	01-12-1994
			DE 69013541	T2	09-03-1995
			DE 69030268	D1	24-04-1997
			DE 69030268	T2	26-06-1997
			DE 386867	T1	29-04-1993
			DK 386867	T3	03-04-1995
			EP 0386867	A2	12-09-1990
			ES 2036978	T1	16-06-1993

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 01/02502

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0586022 A		ES 2098651 T3	01-05-1997
		GR 93300050 T1	30-06-1993
		JP 2291043 A	30-11-1990
		US 5214702 A	25-05-1993

Form PCT/ISA/210 (patent family annex) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/02502

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167

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)
CIB 7 H04N

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 réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	WO 99 07149 A (SCIENTIFIC ATLANTA) 11 février 1999 (1999-02-11) le document en entier	1,2,6-8, 10 11
Y	EP 0 858 184 A (NDS LTD) 12 août 1998 (1998-08-12) le document en entier	11
A	WO 97 04553 A (PHILIPS ELECTRONICS NV ;PHILIPS NORDEN AB (SE)) 6 février 1997 (1997-02-06) page 1, ligne 9 - ligne 16 page 7, ligne 1 - ligne 18 figure 1	1-14
A	US 5 563 950 A (MERZ WILLIAM A ET AL) 8 octobre 1996 (1996-10-08) colonne 1 -colonne 2, ligne 33	1-14

-/--

[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'appartenant 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
30 novembre 2001	06/12/2001

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	Tito Martins, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/02502

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 586 022 A (FISCHER ADDISON M) 9 mars 1994 (1994-03-09) le document en entier	1-14
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW- TECHNICAL,EUROPEAN BROADCASTING UNION. BRUSSELS,BE, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 le document en entier	1-14

1

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 01/02502

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9907149	A	11-02-1999	AU	1581699 A	08-03-1999
			AU	8670598 A	22-02-1999
			AU	8679798 A	22-02-1999
			AU	8679898 A	22-02-1999
			AU	8764298 A	22-02-1999
			AU	8823398 A	22-02-1999
			AU	8823698 A	22-02-1999
			BR	9810967 A	30-10-2001
			BR	9815607 A	13-11-2001
			EP	1010323 A1	21-06-2000
			EP	1010324 A1	21-06-2000
			EP	1010325 A1	21-06-2000
			EP	1013091 A1	28-06-2000
			EP	1000508 A1	17-05-2000
			EP	1000509 A1	17-05-2000
			EP	1000511 A2	17-05-2000
			JP	2001513587 T	04-09-2001
			JP	2001512842 T	28-08-2001
			WO	9907145 A1	11-02-1999
			WO	9907146 A1	11-02-1999
			WO	9907147 A1	11-02-1999
			WO	9907148 A1	11-02-1999
			WO	9907149 A1	11-02-1999
			WO	9909743 A2	25-02-1999
			WO	9907150 A1	11-02-1999
			US	6105134 A	15-08-2000
			US	6292568 B1	18-09-2001
			US	6252964 B1	26-06-2001
			US	2001001014 A1	10-05-2001
			US	6246767 B1	12-06-2001
EP 0858184	A	12-08-1998	IL	120174 A	28-10-1999
			EP	0858184 A2	12-08-1998
			US	6178242 B1	23-01-2001
			GB	2322030 A ,B	12-08-1998
WO 9704553	A	06-02-1997	EP	0793880 A1	10-09-1997
			WO	9704553 A1	06-02-1997
			JP	10505995 T	09-06-1998
US 5563950	A	08-10-1996	US	5559889 A	24-09-1996
			JP	8278750 A	22-10-1996
EP 0586022	A	09-03-1994	US	5005200 A	02-04-1991
			EP	0586022 A1	09-03-1994
			AT	113429 T	15-11-1994
			AT	150605 T	15-04-1997
			AU	620291 B2	13-02-1992
			AU	4242589 A	13-09-1990
			CA	2000400 A1	07-09-1990
			DE	69013541 D1	01-12-1994
			DE	69013541 T2	09-03-1995
			DE	69030268 D1	24-04-1997
			DE	69030268 T2	26-06-1997
			DE	386867 T1	29-04-1993
			DK	386867 T3	03-04-1995
			EP	0386867 A2	12-09-1990
			ES	2036978 T1	16-06-1993

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/02502

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0586022 A		ES 2098651 T3	01-05-1997
		GR 93300050 T1	30-06-1993
		JP 2291043 A	30-11-1990
		US 5214702 A	25-05-1993

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,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,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,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,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZW

(72)発明者 ディエール，エリク
フランス国，３５３４０ リフレ，ラ・ビュザールディエール（番地なし）

Ｆターム(参考) 5C063 AA01 AB03 AB07 AC01 AC05 AC10 CA23 CA36 DA07 DA13 DB10
5C064 BA07 BB02 BC06 BC17 BC18 BC22 BC23 BD02 BD03 BD08 BD09 BD13
5J104 EA16 JA21