[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/14 (2006.01)
H04N 7/24 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480012554.8

[43] 公开日 2006 年 9 月 13 日

[11] 公开号 CN 1833401A

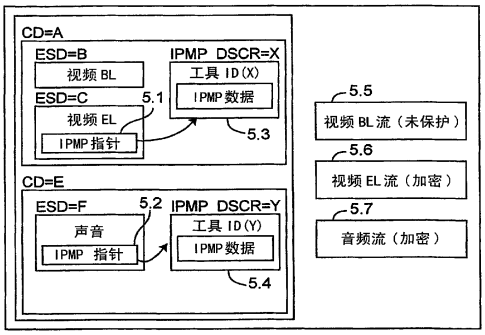
[22] 申请日 2004.4.30
[21] 申请号 200480012554.8
[30] 优先权
[32] 2003. 5. 9 [33] JP [31] 131856/2003
[86] 国际申请 PCT/JP2004/006285 2004.4.30
[87] 国际公布 WO2004/100441 日 2004.11.18
[85] 进入国家阶段日期 2005.11.9
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 吉 明 刘 荆 申省梅 上野孝文
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 江惠民
权利要求书 2 页 说明书 17 页 附图 6 页

[54] 发明名称

被 MPEG－4IPMP 扩展的 ISMA 媒体流的接收装置

[57] 摘要

一种接收被 MPEG－4 IPMP 扩展的 ISMA 媒体流的装置，接收包含有 ISMA 信头、内容、以及表示所述内容的处理方法的 IPMP 工具列表描述符的 ISMA 媒体流，从所述 ISMA 媒体流中取得所述 IPMP 工具列表描述符，检查所述 IPMP 工具列表描述符所表示的工具是否存在于所述接收装置中，在所述工具存在的情况下，利用所述工具处理所述内容，在所述工具不存在的情况下，无故障地结束。



1、一种接收装置，接收被 MPEG－4 IPMP 扩展的 ISMA 媒体流，其中，

接收包含有 ISMA 信头、内容、以及表示所述内容的处理方法的 IPMP 工具列表描述符的 ISMA 媒体流；

从所述 ISMA 媒体中流取得所述 IPMP 工具列表描述符；

检查所述 IPMP 工具列表描述符所表示的工具是否存在于所述接收装置中；

在所述工具存在的情况下，利用所述工具处理所述内容，在所述工具不存在的情况下，无故障地结束。

2、根据权利要求 1 所述的接收装置，其中，

所述 ISMA 媒体流具有 IOD，并从所述 IOD 中取得所述 IPMP 工具列表描述符。

3、一种接收装置，接收被 MPEG－4 IPMP 扩展的 ISMA 媒体流，其中，

接收包含有 ISMA 信头、内容、以及表示所述内容的处理方法的 IPMP 描述符的 ISMA 媒体流；

从所述 ISMA 媒体流中取得所述 IPMP 描述符；

检查所述 IPMP 描述符所表示的工具是否存在于所述接收装置中；

在所述工具存在的情况下，利用所述工具处理所述内容，在所述工具不存在的情况下，无故障地结束。

4、根据权利要求 3 所述的接收装置，其中，

所述 ISMA 媒体流，还包含有指向所述 IPMP 描述符的 IPMP 描述符指针，所述接收装置从所述 ISMA 媒体流中取得所述 IPMP 描述符指针；

取得所述 IPMP 描述符指针所指的地址的所述 IPMP 描述符。

5、根据权利要求 4 所述的接收装置，其中，

从所述 ISMA 媒体流的 ES 描述符中取得所述 IPMP 描述符指针，从所述 ISMA 媒体流的 OD 中取得所述 IPMP 描述符指针所指的所述 IPMP 描述符。

6、根据权利要求 3～5 的任一项所述的接收装置，其中，

在 ISMACryp 解读工具被所述 IPMP 描述符指定的情况下，起动所述 ISMACryp 解读工具，来实施所述内容的解读。

7、根据权利要求 6 所述的接收装置，其中，

从存储于所述 IPMP 描述符中的 ISMACryp_Data 中，取出 ISMACryp 参数；

利用所述被取出的 ISMACryp 参数来设定 ISMACryp 解读工具，并实施所述内容的解读。

8、根据权利要求 6 所述的接收装置，其中，

从所述 ISMA 媒体流的 IPMP 流内的 IPMP 信息中存储的 ISMACryp_Data 中，取出 ISMACryp 参数；

利用所述被取出的 ISMACryp 参数来设定 ISMACryp 解读工具，并实施所述内容的解读。

9、根据权利要求 3 所述的接收装置，其中，

所述 ISMA 媒体流，除了所述 IPMP 描述符，还包含有表示所述至少一个工具的 IPMP 工具列表描述符，

所述接收装置，取得所述 IPMP 工具列表描述符或者所述 IPMP 描述符后，检查所述 IPMP 工具列表描述符或者所述 IPMP 描述符所表示的工具是否存在于所述接收装置中。

被 MPEG－4 IPMP 扩展的 ISMA 媒体流的接收装置

技术领域

本发明，涉及针对 ISMA 保护框架可互换的 MPEG－4 IPMP 扩展。

背景技术

这几年来，在媒体内容流通领域，保证通过互联网的视频和声音的配送被广泛推进。各种标准化组织为了提供对该问题的解决对策而做出了很大的努力。互联网流媒体联盟（ISMA：Internet Streaming Media Alliance）即是这种组织之一。为了满足这个需求，提出了可供提供商构筑能在 IP 框架以及互联网中使用的视频和音声系统时使用的、使用现有的开放标准的框架。虽然该规格中假定使用现有的 MPEG 技术，并主要把焦点集中于现阶段的 MPEG－4 技术上，但也预备在将来实施包含 MPEG－2 和 MPEG－7 技术的变更和修正。

ISMA 还规定有 ISMA 媒体流用的加密框架，即 ISMACryp。该框架，可对新的媒体编码进行扩展，并可对应于新的加密，而且也可应用于各种加密密钥管理、安全、或数字权利管理（DRM）系统。其还规定面向 ISMA 规格的媒体流以及媒体信息的认证用的缺省加密方式。图 1 中表示 ISMA 框架用的 ISMACryp 保护的构架图。图 1 的 ISMA DRM 的范围，为 ISMA 媒体的加密以及 ISMA 信息的认证，在图中被标记作“ISMACryp”，ISMACryp 的信令（signaling）被标记作“RTSP/SDP＋”（ISMA1.0 SDP 定义・加 ISMACryp 信令）。主管（1.1）负责内容的准备和发行。用于密钥/许可管理界面的协议，位于 ISMACryp 范围之外。另外，在图 1 中，从密钥/许可管理往 ISMA 接收机的密钥（或许可）的配送，位于 ISMACryp 的范围之外。一般认为，ISMACryp 技术开发的目的在于，提供将上述这种信息配送到终端的安全的方法。发送机（1.2），通过被称作“ISMACryp”的开放标准的协议，来负责往 ISMA 接收机的配送，其中，“ISMACryp”

由 ISMA 发送机使用 RTSP/SDP＋（ISMA1.0 SDP 定义・加 ISMACryp 信令）来告知（signal）、或者利用第 3 装置告知。

在 ISMA DRM 构架中，ISMA 接收机能够处理被 ISMACryp 加密的流、被认证的信息、以及信令。“ISMACryp”，是提供具备 ISMA1.0 媒体及加密、信息认证、整体服务的协议的技术。

图 2 是更详细地表示 ISMA 接收机的构架的图，包括密钥/许可管理（KEY MGT）、RTSB 控制接口、以及作为 ISMA 数据用的加密服务的面向 ISMACryp 的接口。ISMACryp 接收机，能够对 ISMA 数据进行加密、进行认证，并检查其完全性。

图 3 是表示流被管理成文件、或者编码后被直接提供给网络的 ISMACryp 环境的图。虽然在任何一种情况下，均在配送之前被加密，但信息认证在配送时进行。在接收机（媒体再生机/解码器）中，流被播放器、或现金服务器（cash server）下的个人录像机等的文件接收，或直接被解码器所接收。ISMACryp 变换由编码器/发送机进行，并且解读由终结于解码器/接收机的弧（arc）进行。

按照 ISMA 的宣称，以两种接收机、即 ISMA 专用接收机和 MPEG 系统对应接收机为对象。这里，所谓“ISMA 专用接收机”，定义为不对应 MPEG－4 系统、即不能够完全处理与 MPEG－4 信号通知（signaling）和 MPEG－4（基本）媒体流相关的控制（基本）流的接收机。与此相对，“MPEG 系统对应接收机”，不仅能够处理 ISMA 关联信息，还能够处理 MPEG－4 系统层信息。和 MPEG 系统对应接收机的相互运用可能性，通过至少传输最小限的 MPEG 系统信令的 MPEG IOD（初始目标描述）来实现。IOD 被作为二进制 SDP（会话描述协议）属性、即 SDP IOD 包含。

ISMACryp，还能够应用于双方类型的接收机。扩展 SDP 信息内的二进制 IOD。新的信令，相比 ISMA 信令中显现的冗长度，更注重非对称性。提供 SDP IOD 的“最小”以及“基本”信令参数，来使接收机的与 MPEG－4 IPMP 系统的相互运用性最大化。

然而，现有的 ISMACryp 规定下的 IOD 的扩展并不完全，且与最新的 MPEG－4 IPMP 扩展标准没有一致性。其结果，可能会存在 ISMA 流不能被 MPEG－4 IPMP 扩展互换接收机正确识别的情况。例如，ISMACryp 标

准中规定，使用 IOD 内的 IPMP_Descriptor 的存在来告知 ISMACryp 保护。但是，若根据 MPEG－4 IPMP 扩展，在存在 IPMP 保护时，应当在 IOD 内提示工具列表描述符。这些不完全性和不一致性，很有可能妨碍 ISMA 框架的与 MPEG－4 IPMP 扩展互换接收机的相互运用性。

发明内容

本发明要解决以下课题。

ISMACryp 标准，通过借助 SDP 内的 IOD 扩展来使用 MPEG－4 IPMP，规定 ISMACryp 保护的信令。IOD 内的 IPMP_Descriptor 的存在，对接收机告知该媒体流正被保护。对于 MPEG IPMP 非互换接收机的情况，允许以独自且适当的方法来处理流。例如，简单地忽略流。可是，MPEG－4 IPMP 扩展标准规定，应该在 IOD 内提示工具列表描述符来表示 IPMP 保护。标准中，不保证为了 IPMP 保护而在 IOD 内存在 IPMP_Descriptor。因此，在由 ISMACryp 所规定的信令方法中，可能无法对 IOD 含有工具列表描述符而不含 IPMP_Descriptor 的媒体流被保护的机制进行正确地检测。

再有，为了使 MPEG－4 IPMP 扩展互换的接收机能够接收与 ISMA 相关的数据，例如，伴随 IPMP 数据的加密信息和 KMS 结构，ISMACryp 标准基于 MPEG－4 IPMP 标准，用自己规定的 ISMACryp_Descriptor 扩展 IOD 内的 IPMP_Descriptor。但是，由于 MPEG－4 IPMP 标准的更替较为快速，IOD 的语法被变更后，与基于 ISMACryp 标准的旧版本不同。由此带来的问题是，存储于 IPMP 上下文（context）内的 ISMA 关联数据可能无法被与最新的 MPEG－4 IPMP 扩展标准兼容的接收机识别。为了将已经规定完毕的 ISMA 参数的变更保持最小，同时保持最新的 MPEG－4 IPMP 扩展标准的一贯性，需要能够用现有 MPEG－4 IPMP 扩展标准存储 ISMA 关联数据的新的机制，并要求该机制与 MPEG－4 IPMP 扩展标准的旧版本具有后方互换性（backward compatibility：向后兼容性）。

本发明的目的在于，提供一种对于 ISMA 保护框架可互换的 MPEG－4 IPMP 扩展。

本发明为了解决信令的问题，规定告知 MPEG 初始对象描述符（IOD）中的 ISMACryp 保护的存在的信令机构。使用工具列表和 IPMP 描述符来

告知保护。该方法与最新的 MPEG－4 IPMP 扩展标准具有兼容性，同时最大限度地提供与 MPEG 系统对应 ISMA 接收机的兼容性。另外，提供用于识别再生内容所需的工具的灵活方法。

本发明还规定了存储 ISMACryp 参数并变换为 MPEG 系统对应 ISMA 接收机用的机制。能够从由 MPEG－4 IPMP 扩展规定的 IPMP_Data_BaseClass 中扩展 ISMA 专用 Cryp_Data ，存储 ISMACryp 参数。

本发明中的接收被 MPEG－4 IPMP 扩展的 ISMA 媒体流的装置，

接收包含有 ISMA 信头、内容、以及表示所述内容的处理方法的 IPMP 工具列表描述符的 ISMA 媒体流；

从所述 ISMA 媒体流中取得所述 IPMP 工具列表描述符；

检查所述 IPMP 工具列表描述符所表示的工具是否存在于所述接收装置中；

在所述工具存在的情况下，利用所述工具处理所述内容，在所述工具不存在的情况下，无故障地结束。

另外所谓“无故障地结束”，意思是进行预定的处理后结束。所谓“故障”表示例如“挂起”。

另外，所述 ISMA 媒体流具有 IOD，并从所述 IOD 中取得所述 IPMP 工具列表描述符。

再有，本发明中的接收被 MPEG－4 IPMP 扩展的 ISMA 媒体流的装置，

接收包含有 ISMA 信头、内容、以及表示所述内容的处理方法的 IPMP 描述符的 ISMA 媒体流；

从所述 ISMA 媒体流中取得所述 IPMP 描述符；

检查所述 IPMP 描述符所表示的工具是否存在于所述接收装置中；

在所述工具存在的情况下，利用所述工具处理所述内容，在所述工具不存在的情况下，无故障地结束。

另外，优选所述 ISMA 媒体流，还包含有指向所述 IPMP 描述符的 IPMP 描述符指针，所述接收装置从所述 ISMA 媒体流中取得所述 IPMP 描述符指针，

取得所述 IPMP 描述符指针所指的地址的所述 IPMP 描述符。

再有，也可从所述 ISMA 媒体流的 ES 描述符中取得所述 IPMP 描述符指针，从所述 ISMA 媒体流的 OD 中取得所述 IPMP 描述符指针所指的所述 IPMP 描述符。

另外，也可在 ISMACryp 解读工具被所述 IPMP 描述符指定的情况下，起动所述 ISMACryp 解读工具，来实施所述内容的解读。

再有，也可构成为，从存储于所述 IPMP 描述符中的 ISMACryp_Data 中，取出 ISMACryp 参数；

利用所述被取出的 ISMACryp 参数来设定 ISMACryp 解读工具，并实施所述内容的解读。

再有，还可构成为，从所述 ISMA 媒体流的 IPMP 流内的 IPMP 信息中存储的 ISMACryp_Data 中，取出 ISMACryp 参数；

利用所述被取出的 ISMACryp 参数来设定 ISMACryp 解读工具，并实施所述内容的解读。

另外，也可构成为，所述 ISMA 媒体流，除了所述 IPMP 描述符，还包含有表示所述至少一个工具的 IPMP 工具列表描述符，

所述接收装置，取得所述 IPMP 工具列表描述符或者所述 IPMP 描述符后，检查所述 IPMP 工具列表描述符或者所述 IPMP 描述符所表示的工具是否存在于所述接收装置中。

此处，在 ISMA 框架内构筑 IOD 和 OD。IPMP 工具列表描述符被嵌入到 IOD 内，若 ISMACryp 保护存在，则在 IOD 和 OD 内嵌入 IPMP 描述符指针和 IPMP 描述符。

通过 SDP IOD 信令来将 IOD 和 OD 运送到理解 MPEG－4 系统的 ISMA 接收机。接收机解析 IOD 和 OD。若检测到 IPMP 工具列表，接收机识别出存在 ISMACryp 保护。若检测到 IPMP 描述符指针和 IPMP 描述符，接收机能够识别出哪个流被哪个工具保护。

ISMA 框架内，在流被 ISMACryp 保护的情况下，ISMACryp 参数（例如，密码识别符）被存储于 ISMACryp_Data，能够添加到 IPMP 描述符或 IPMP 流内。参数的存储以 MPEG－4 IPMP 扩展为标准。

在接收机侧，能够在保持与 MPEG－4 IPMP 扩展兼容的同时，从 IPMP

描述符或 IPMP 流中取出 ISMACryp 用的参数。接着，能够使用此参数来设定 ISMACryp 解读工具。

通过使用本发明，ISMA 保护框架能够实现与 MPEG－4 IPMP 扩展互换接收机的相互运用。

本发明利用 IOD 内的工具列表以及 OD 内的 IPMP 描述符来告知 ISMACryp 保护。藉此，信令方法能够灵活地实现，并真正与最新的 MPEG－4 IPMP 扩展标准兼容，从而使得 MPEG 系统对应 ISMA 接收机能够相互运用。

本发明还生成从 IPMP_Data_BaseClass 扩展得到的 ISMACryp_Data。利用本发明中的 ISMACryp_Data，能够存储 ISMACryp 参数，并且能够连续地存储于 IPMP 描述符或 IPMP 流中的其中之一。ISMACryp 参数的存储，目前正在成为 MPEG－4 IPMP 扩展遵守事项。

附图说明

图 1 是表示 ISMACryp 构架的图。

图 2 是表示 IPMPCryp 接收机的构架的图。

图 3 是表示使用 IPMPCryp 的保护的终端间流程的图。

图 4 表示 MPEG－4 IPMP 扩展内容结构。

图 5 是表示使用 IPMP 描述符的保护信令的图。

图 6 是表示导入到 SDP 内的 IOD 中的 IPMP 信息的图。

图 7 是 ISMA 接收机中的 IPMP－X 处理的流程图。

具体实施方式

IPMP 扩展信令

现行 ISMACryp，对应于面向 ISMA 专用及 MPEG 接收机的 SDP IOD 信令（signaling）。虽然 ISMA 专用接收机，仅受理 SDP FMTP 信令参数，但是 SDP IOD 的流被 ISMACryp 保护（最小 IPMP 信令），对任何 MPEG 接收机都必须作出信令。KMS，可以仅利用 SDP IOD 内的 IPMP 信令（基本 IPMP 信令），来对 ISMACryp 作出信令。

在本说明书中，提供与 MPEG－4 IPMP 扩展兼容的语法。ISMACryp

能够以最小的付出，容易地实现与 MPEG－4 IPMP 扩展的兼容，并且还提供灵活的保护方案。

最小 IPMP－X 信令

IPMP 扩展，规定 IOD 中的 IPMP 工具列表（tool list）描述符。工具列表描述符，对后面出现的流列所必要的 IPMP 工具的列表进行识别。根据 MPEG－4 IPMP 扩展，在存在 IPMP 保护时，应该在 IOD 内提示工具列表描述符。因此，在最小限的 IPMP－X 信令的情况下，为了达到该目的，提出使用 IOD 内的 IPMP 工具列表描述符替代 IPMP 描述符。

用 SDP 导入到 MPEG－4 IOD 中的、IOD 中的 IPMP 工具列表的位置，在图 6 中作为 6.1 表示。

根据指定加密和 KMS 信息转送的现行的 ISMACryp 规格，应该在 MPEG IPMP 工具列表描述符中提示至少两个工具。首先是 KMS 工具，另一个是 ISAM 解读工具。MPEG IPMP 工具列表中的 ISMACryp 工具的存在，告知 ISMACryp 保护。

表 1 表示具有 ISMACryp 工具的工具列表描述符的示例。

表 1

	IPMP_ToolListDescriptor		
1	8	IPMP_ToolListDescTag	0x60
2	16	描述符的大小	
		IPMP_Tool	
3	8	IPMP_ToolTag	0x61
4	16	描述符的大小	
5	128	IPMP_ToolID	值由各服务提供商分配给自身的 KMS 工具
6	1	isAltGroup	0
7	1	isParametric	0
8	6	预留	0b0000.00
9	8	工具 URL 的大小	
10		工具 URL	
		IPMP_Tool	
11	8	IPMP_ToolTag	0x61
12	16	描述符的大小	
13	128	IPMP_ToolID	值分配给 ISMA 解读工具
14	1	isAltGroup	0
15	1	isParametric	0
16	6	预留	0b0000.00
17	8	工具 URL 的大小	
18		工具 URL	

IPMP 工具列表，由图 4 所示的 MPEG－4 IPMP 扩展内容结构表示。通过使用 IPMP 工具列表（4.1），不仅能够容易地作出 ISMACryp 保护存在的信令，还能够极灵活地进行工具的识别。工具列表下的 IPMP 工具，可由三种方法识别。第一种方法是，使用值由公共注册机构分配的固定 128 位 IPMP_Tool ID（4.2）。第二种方法是，使用表示作为彼此等同的替代物的工具的 IPMP_Tool ID（4.3）的列表。如此，终端能够更灵活地实施自

身的工具选择。最后的方法是，使用用于描述 IPMP 工具应该满足的基准的参数标注（4.4），而这种情况下，终端用于执行必要的功能的工具选择的自由度变大。

基本 IPMP－X 信令

在 MPEG 系统对应接收机的情况下，与进行 IPMP 关联的处理相比，需要更多的 IPMP 信息。作为更高性能的 MPEG IPMP 扩展信令的基础，使用以下的 IPMP－X 信令。将第二部分中介绍的工具列表与 MPEG 互换接收机所必要的基础信息一同提供。对被加密的基本流，对应的 ES 描述符必须包含有以下的 IPMP_DescriptorPointer（表 2）。

表 2

描述符名			
区域编号	位大小	区域名	值
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	描述符大小	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPX_DescriptorID	0x0002/0x0003
5	16	IPMP_ES_ID	0x0000

图 5 表示该 IPMP 扩展保护信令的概念。通过 ES_Descriptor 内的该描述符指针（5.1 和 5.2）存在，表示被与该描述符相关联的流，是被参照 IPMP_Descriptor（5.3 和 5.4）所指定的 IPMP 工具保护和管理的对象。表 3 表示的参照 IPMP_Descriptor，应被存储在目标描述符中。

表 3

描述符名			
区域编号	位大小	区域名	值
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	描述符大小	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002/0x0003
6	128	IPMP_ToolID	值分配给 ISMA 解读工具
7	8	控制点代码	0x01（解读缓存和解读器之间）
8	8	序列代码	0x80

另外，IOD 必须包含以下的 IPMP_ DescriptorPointer（表 4）。在以下的示例中，可知由参照描述符表示的特定的 DRM 工具（加密密钥管理系统），需要在全局范围（global-scope）内生成（intance-generated）。

表 4

描述符名			
区域编号	位大小	区域名	值
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	描述符大小	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDEx	0x0001
5	16	IPMP_ES_ID	0x0000

上述的 IPMP_ DescriptorPointer，指示 IPMP_DescriptorIDEx 为 0x0001 的 IPMP_Descriptor。接下来，被指定的 IPMP_Descriptor 必须被在 IOD（表

5）中提示。需要留意的是，在 KMS 的情况下，描述符的控制指针应当设定为 0x00，以表示是在全局范围内。

表 5

描述符名			
区域编号	位大小	区域名	值
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	描述符大小	22
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0001
6	128	IPMP_ToolID	值由各服务提供商分配给 KMS 工具
7	8	控制点代码	0x00（无控制指针）

用与 IPMP 扩展兼容的方法存储 ISMACryp

ISMACryp 用参数组描述流的加密。以下列示参数组。

表 6

参数	值	含义	缺省
Crypto-suite	1..255	密码、模式、密钥长度等	1 [1)]
IV-length	1..8	IV 的字节单位的长度	4
Delta-IV-length	0..2	DeltaIV 的字节单位的长度	0
Selective-encryption	0..1	在选择性地加密流时设定为‘1’	0
Key-indicator-per-AU	0..1	在信息包中出现多个密钥指示符时，设定为‘1’	0
Key-indicator-length	0..255	密钥指示符的字节单位的长度	0

1）第 10.0 部分的 AES－CTR 缺省

由于用与 IPMP 扩展兼容的方法存储参数，因此 ISMACryp_Data 可从 IPMP－X 所规定的 IPMP_Data_BaseClass 中扩展。IPMP_Data_BaseClass 如下所示，由 MPEG－4 IPMPX 规定。

```
abstract aligned(8) expandable(2^28－1) class IPMP_Data_BaseClass:
    bit(8) tag=0 .. 255
{
    bit(8)    Version;
    bit(32)   dataID;
    //Field and data extending this message.
}
```

ISMACryp_Data，可用用户所定义的标签从上述的基类（base class）扩展。接下来，数据可以具有用于存储参数的自身的区域组。从而，保证解释相同内容流的不同类型的 ISMA 终端的兼容性。

此 ISMACryp_Data，能够以标准的方法存储于两个位置。第一，存储到 IPMP 描述符中。表 7 表示具有该 ISMACryp_Data 的 IPMP 描述符的示例。

表 7

描述符名			
区域编号	位大小	区域名	值
		IPMP_Descriptor	
1	8	IPMP_ Descriptor tag	11
2	8	描述符大小	23
3	8	IPMP_ DescriptorID	0xFF
4	16	IPMP_ Type	0xFFFF
5	16	IPMP_ DescriptorIDEx	0x0002/0x0003
6	128	IPMP_ToolID	值分配给 ISMA 描述符工具
7	8	控制点代码	0x01（解读缓存和解读器之间）
8	8	序列代码	0x80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	规定预留
8	8	数据大小	20
9	8	密码的组	密码识别符
11	4	IV-length	初始化向量的字节长度
12	2	Delta-IV-length	AU 基的 IV 的字节长度
13	1	Selective-encryption	使用选择性加密时为 1
14	1	Key-indicator-per-Au	在信息包中出现多个密钥指示符在时为 1
15	8	Key-indicator-length	密钥指示符的字节长度

用 SDP 导入到 MPEG－4 IOD 内的 IPMP 描述符的 OD 流中的位置，在图 6 中作为符号 6.1 表示。

存储 ISMACryp_Data 的第二方法是，作为 IPMP_Message 内的净荷来存储，从而如 MPEG－4 IPMP 扩展所规定的那样，连续地存储于 IPMP 流中。

aligned (8) expandable(228－1) class IPMP_Message

{

```
        bit(16)     IPMPS_Type;
        if (IPMPS_Type==0)
        (
          bit (8) URLString[sizeOfInstance-2];
        )
        else (if (IPMPS_Type  ==0x0001)
        (
          bit(16) IPMP_DescriptorID;
           IPMP_Data_BaseClass IPMP_ExtendedData[]
        }else {
          bit(8) IPMP_data[sizeOfInstance-2];
        }
    }
```

表 8 表示 IPMP_Message 存储 ISMACryp_Data 时的语法。由具有该 IPMP_DescriptorIDEx 的 IPMP 描述符所指定的 IPMP 工具，是 IPMP_Message 的发送目的地。

表 8

区域编号	位大小	区域名	值
		IPMP_Message	
1	16	信息大小	
2	16	IPMPS_ Type	0x0001
3	16	IPMP_ DescriptorIDEx	
		ISMACryp_Data	
4	8	ISMACryp_DataTag	规定预留
5	8	数据大小	20
6	8	密码组	密码识别符
7	4	IV-length	初始化向量的字节长度
8	2	Delta-IV-length	AU 基的 IV 的字节长度
9	1	Selective-encryption	使用选择性加密时为 1
10	1	Key-indicator-per-Au	在信息包中出现多个密钥指示符时为 1
11	8	Key-indicator-length	密钥指示符的字节长度

ISMA 接收机中的 IPMPX 信令的处理

按照上述 IPMPX 信令，在 ISMA 接收机中，能够指定流是否被保护，在被保护的情况下，能够指定实施什么样的处理。

在获取描述被 ISMA 接收机关联的媒体流的 SDP 参数（S01）的情况下，检查是否存在被称作 MPEG－4 IOD 的属性（S02），在其存在的情况下，可知此被关联的媒体流是与 MPEG－4 系统兼容的流。在不存在的情况下，以非 MPEG 方法进行处理（S03）。接下来，检查在 MPEG－4 IOD 内是否存在 IPMP 工具列表（S04）。在 MPEG－4 IOD 内存在 IPMP 工具列表的情况下，可知该媒体流被用 IPMP 扩展保护。然后，按照 IPMP 描述符所指定的 Tool_ID 来激活工具（S06）。激活 KMS 工具来处理密钥管理问题，并且激活密码解读工具来在特定的控制点处理媒体流的密码解读（S07）。另外，检查导入到 IPMP 描述符或 IPMP 流中的 ISMACryp_Data 是否存在（S08），并且在其存在的情况下，将其配送给密码解读工具，并

进行设定（S09）。再有，上述步骤 S04，在不存在 IPMP 工具列表的情况下，用没有 IPMP 保护的 MPEG 方法进行处理（S05）。图 7 示出了上述过程。

另外，本发明能够采用各种实施方式所示的以下结构。按照第一结构，是在 ISMA 接收机一侧，使用 MPEG－4 IPMP 扩展来实施 ISMA 媒体流的灵活保护的装置，包括：

从 IOD 接收 IPMP 工具列表描述符的步骤；

检查工具列表所表示的工具，在用工具 ID 识别出的 ISMACryp 解读工具存在的情况下，检查所述 ISMACryp 解读工具是否存在，并且在不存在的情况下，接收机无故障地拒绝接收的步骤；以及，

检查工具列表所表示的工具，在用工具 ID 识别出的 ISMACrypKMS 工具存在的情况下，检查 ISMACrypKMS 工具是否存在，并且在不存在的情况下，接收机无故障地拒绝接收的步骤。

按照第二结构，是在上述记载的 ISMA 接收机侧，使用 MPEG－4 IPMP 扩展来实施 ISMA 媒体流的灵活保护的装置，检查所述 IPMP 工具列表的步骤，包括：

从 ES 描述符中接收 IPMP 描述符指针，并从 OD 中接收参照 IPMP 描述符的步骤；以及，

在 ISMACryp 解读工具被 IPMP 描述符指定的情况下，起动 ISMACryp 解读工具，并根据所述 ES 描述符的描述，开始被保护的媒体流的解读的步骤。

按照第三结构，是在上述记载的 ISMA 接收机侧，使用 MPEG－4 IPMP 扩展来实施 ISMA 媒体流的灵活保护的装置，检查所述 IPMP 工具列表的步骤，包括：

从 ES 描述符中接收 IPMP 描述符指针，并从 OD 中接收参照 IPMP 描述符的步骤；

在 ISMACryp 解读工具被 IPMP 描述符指定的情况下，起动 ISMACryp 解读工具的步骤；

从被存储于 IPMP 描述符中的 ISMACryp_Data 中取出 ISMACryp 参数的步骤；以及，

使用所述被取出的ISMACryp参数，来设定ISMACryp解读工具，并参照所述ES描述符来开始被保护的媒体流的解读的步骤。

按照第四结构，是在上述记载的ISMA接收机侧，使用MPEG－4 IPMP扩展来实施ISMA媒体流的灵活保护的装置，检查所述IPMP工具列表的步骤，包括：

从ES描述符中接收IPMP描述符指针，并从OD中接收参照IPMP描述符的步骤；

在ISMACryp解读工具被IPMP描述符指定的情况下，起动ISMACryp解读工具的步骤；

从IPMP流内的IPMP信息中所存储的ISMACryp_Data中，取出ISMACryp参数的步骤；以及，

使用所述被取出的ISMACryp参数来设定ISMACryp解读工具，并参照所述ES描述符来开始被保护的媒体流的解读的步骤。

如上所述，虽然通过优选的实施方式对本发明进行了详细说明，但是本发明不限于此，本领域的技术人员了解，在记载于权利要求书中的本发明的技术范围内，可以实现很多的优选变形例和修正例。

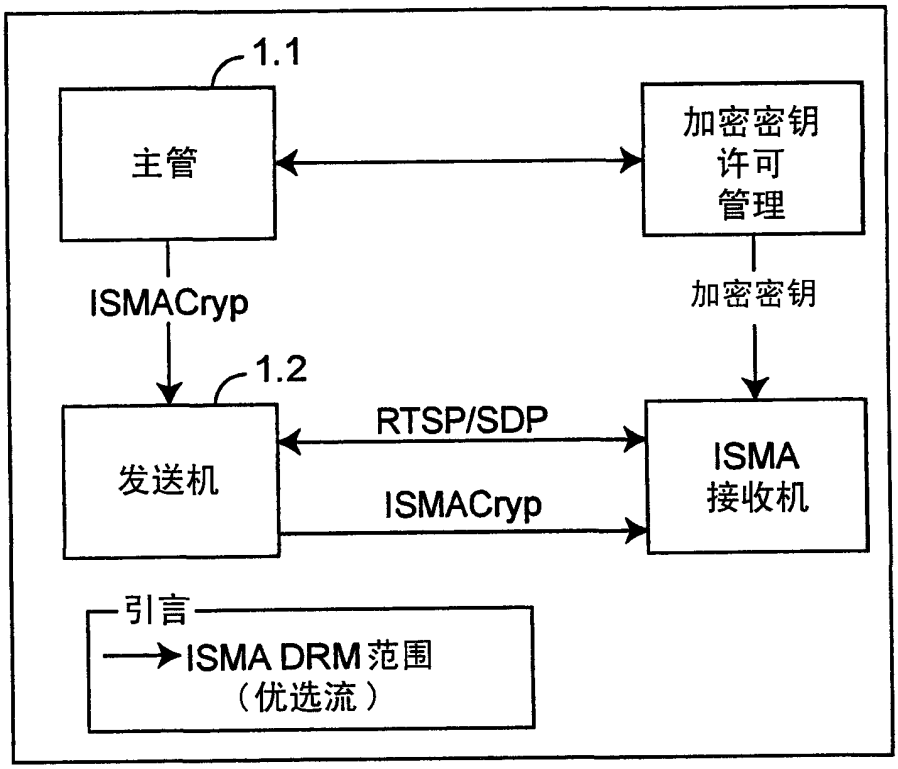

1.1
主管
加密密钥
许可
管理
ISMACryp
加密密钥
1.2
发送机
RTSP/SDP
ISMACryp
ISMA
接收机
引言
ISMA DRM范围
（优选流）

图 1

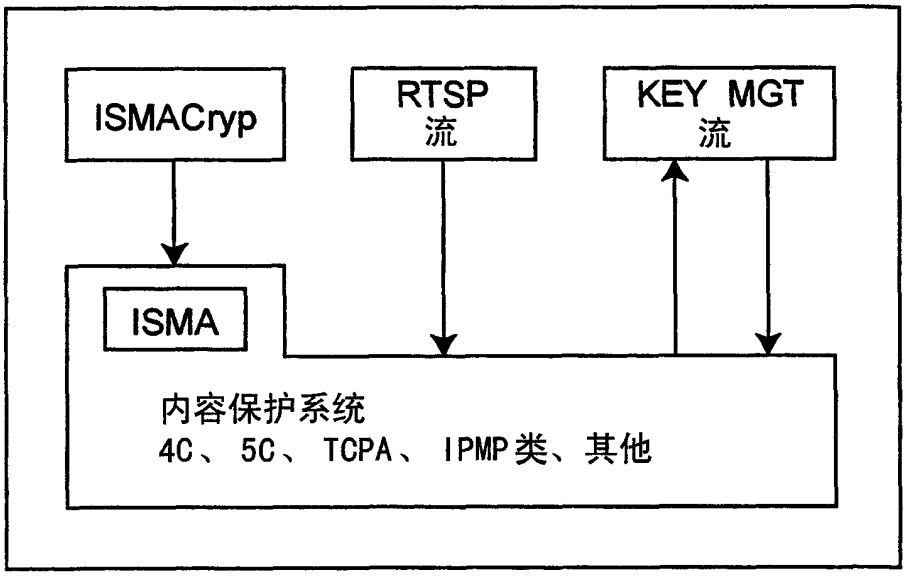

ISMACryp
RTSP
流
KEY MGT
流
ISMA
内容保护系统
4C、 5C、 TCPA、 IPMP类、其他

图 2

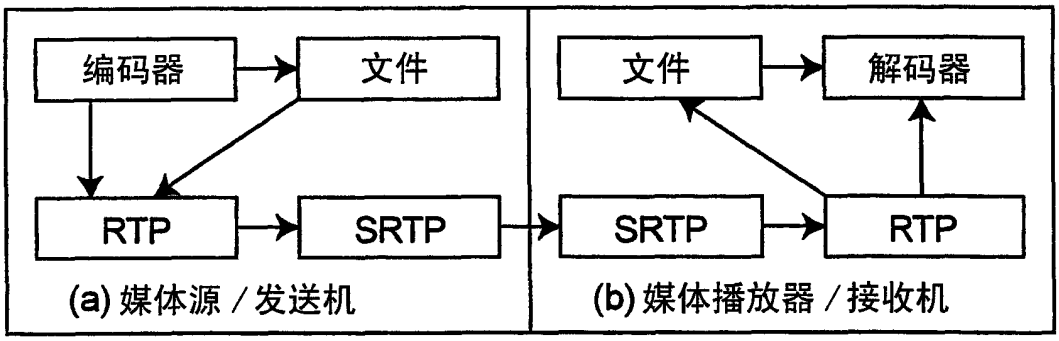

编码器
文件
RTP
SRTP
(a) 媒体源 / 发送机
文件
解码器
SRTP
RTP
(b) 媒体播放器 / 接收机

图 3

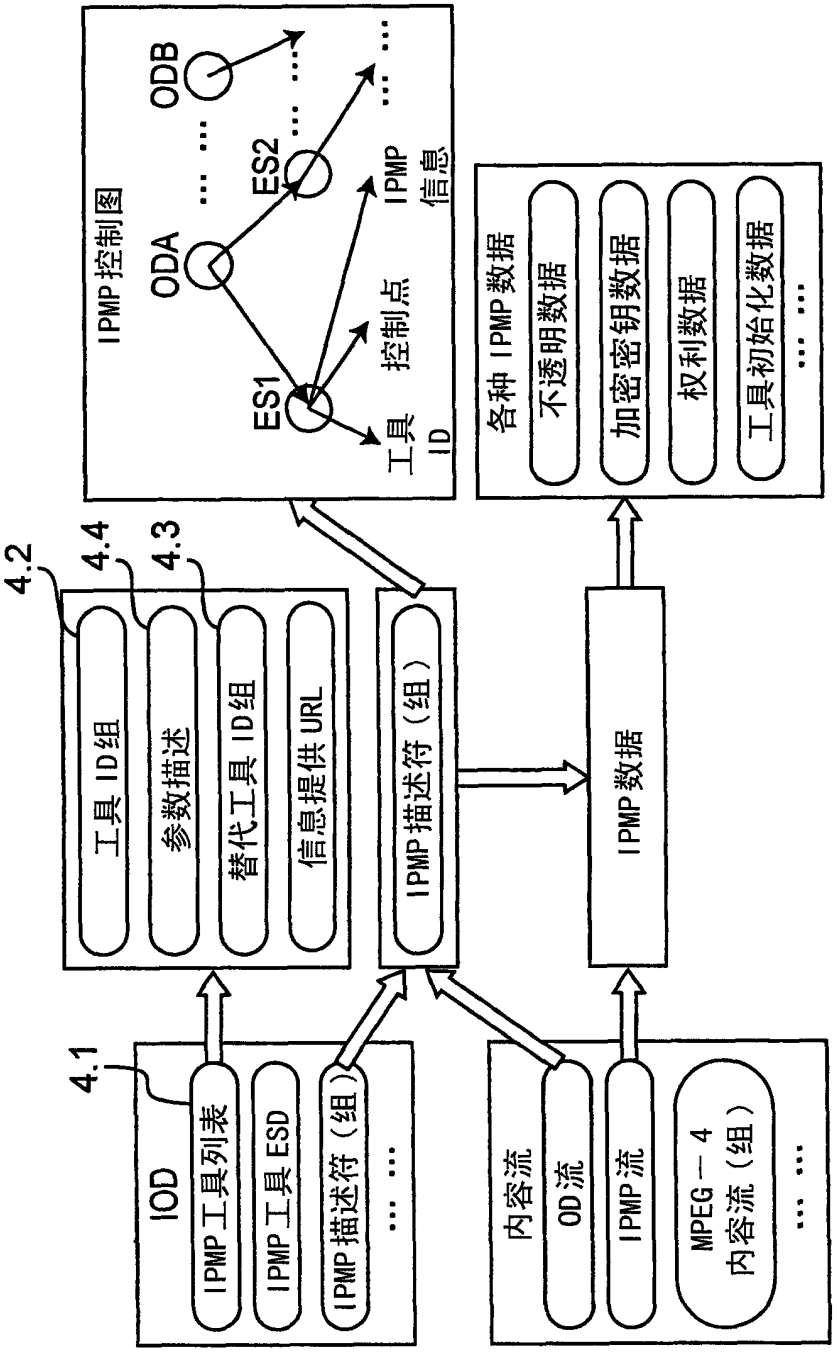

IPMP控制图
ODB
ODA
ES2
ES1
工具 ID
控制点
IPMP 信息
各种 IPMP数据
不透明数据
加密密钥数据
权利数据
工具初始化数据
4.2
4.4
4.3
工具 ID组
参数描述
替代工具 ID组
信息提供 URL
IPMP描述符（组）
IPMP数据
4.1
IOD
IPMP工具列表
IPMP工具 ESD
IPMP描述符（组）
内容流
OD流
IPMP流
MPEG－4 内容流（组）

图 4

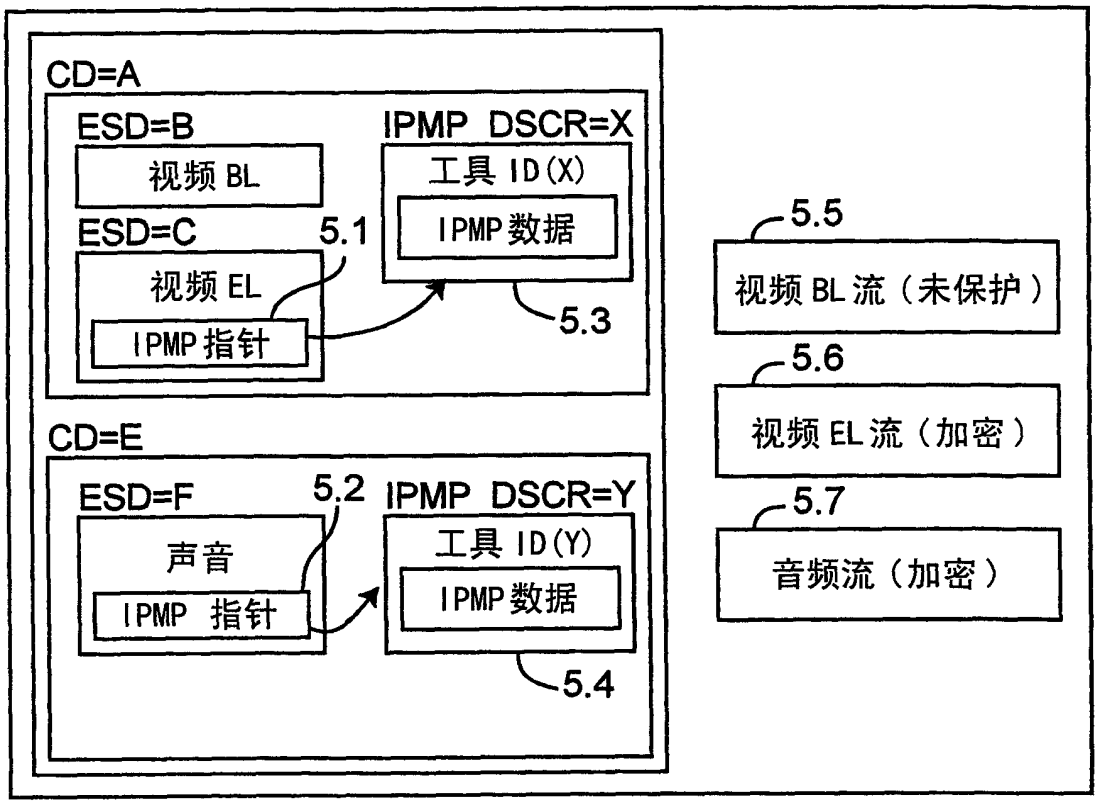

CD=A
ESD=B
视频 BL
ESD=C
视频 EL
IPMP 指针
5.1
IPMP DSCR=X
工具 ID(X)
IPMP 数据
5.3
CD=E
ESD=F
声音
IPMP 指针
5.2
IPMP DSCR=Y
工具 ID(Y)
IPMP 数据
5.4
5.5
视频 BL 流（未保护）
5.6
视频 EL 流（加密）
5.7
音频流（加密）

图 5

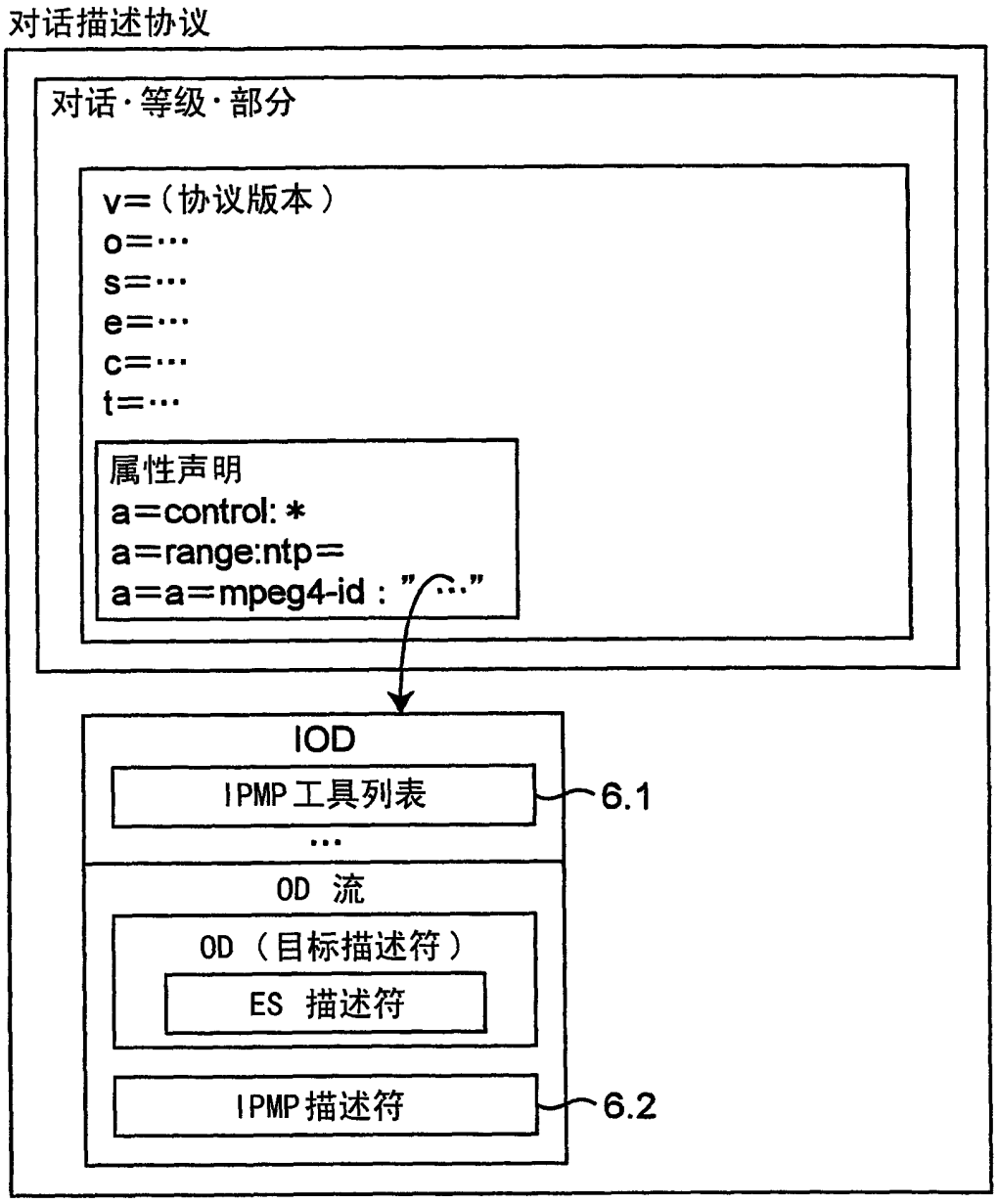

对话描述协议
对话·等级·部分
v=（协议版本）
o=…
s=…
e=…
c=…
t=…
属性声明
a=control:*
a=range:ntp=
a=a=mpeg4-id：”…”
IOD
IPMP工具列表
6.1
…
OD 流
OD（目标描述符）
ES 描述符
IPMP描述符
6.2

图 6

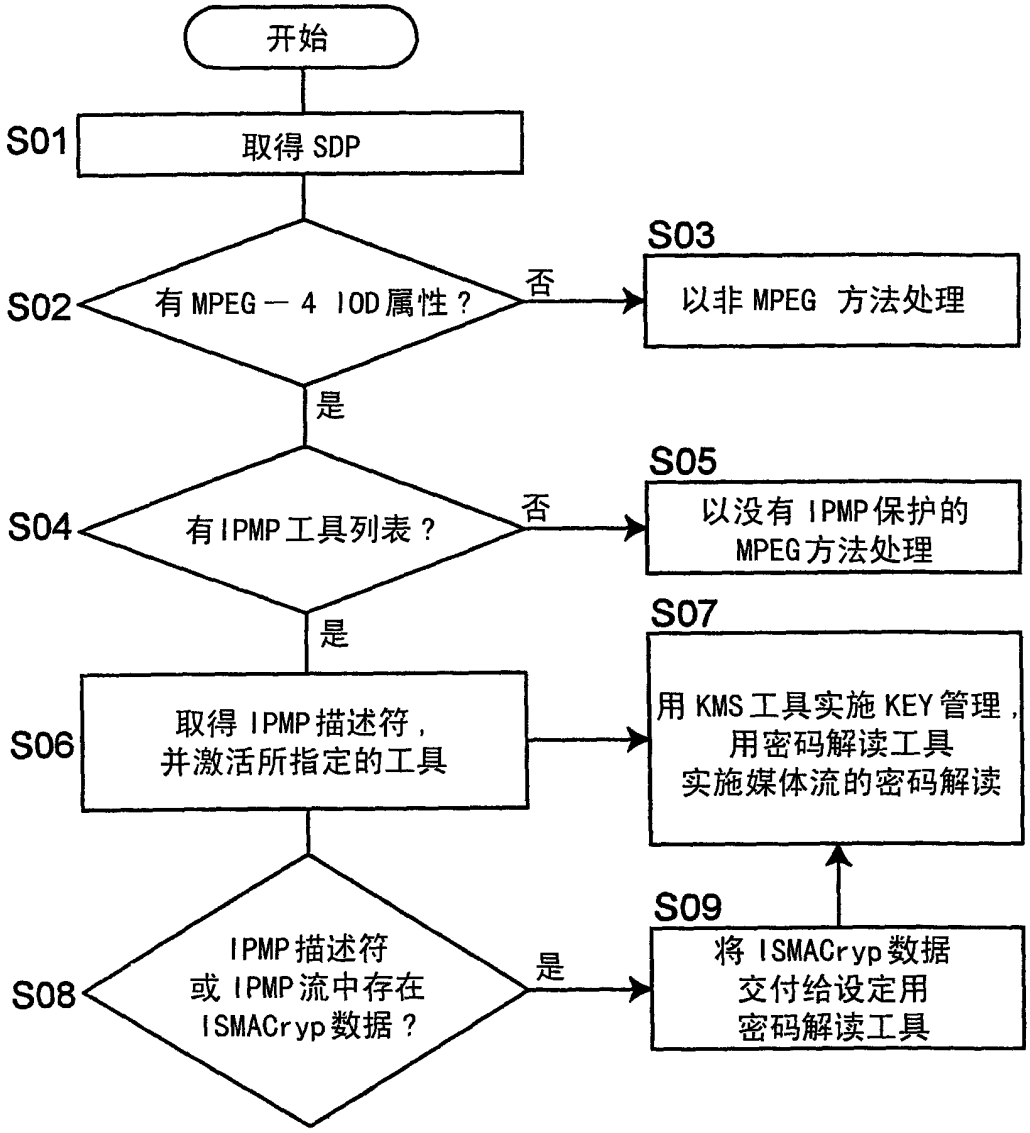

开始
S01
取得 SDP
S02
有 MPEG－4 IOD属性？
否
S03
以非 MPEG 方法处理
是
S04
有IPMP工具列表？
否
S05
以没有 IPMP保护的
MPEG方法处理
是
S06
取得 IPMP描述符，
并激活所指定的工具
S07
用 KMS工具实施 KEY管理，
用密码解读工具
实施媒体流的密码解读
S08
IPMP描述符
或 IPMP流中存在
ISMACryp数据？
是
S09
将 ISMACryp数据
交付给设定用
密码解读工具

图 7