[19] 中华人民共和国国家知识产权局

[12] 发明专利说明书

专利号 ZL 200610114900.4

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 9/08 (2006.01)
H04N 5/91 (2006.01)
H04N 5/44 (2006.01)
H04N 7/16 (2006.01)

[45] 授权公告日 2010 年 3 月 3 日

[11] 授权公告号 CN 100593295C

[22] 申请日 2006.8.16
[21] 申请号 200610114900.4
[30] 优先权
[32] 2005. 8.16 [33] JP [31] 2005 - 235639
[73] 专利权人 索尼株式会社
地址 日本东京
[72] 发明人 小方一郎
[56] 参考文献
EP1073222A2 2001.1.31
US2004/0052377A1 2004.3.18
US4926475 1990.5.15
审查员 杜 军

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 党建华

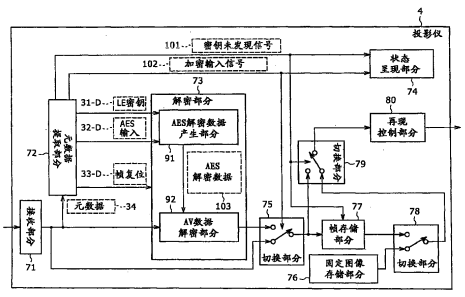
权利要求书 5 页 说明书 41 页 附图 14 页

[54] 发明名称

发送/接收系统、发送/接收方法、接收设备、接收方法和程序

[57] 摘要

公开了一种发送/接收系统、发送/接收方法、接收设备、接收方法和程序。 本发明提供了包含第一发送设备、第二发送设备和接收设备的发送/接收系统。 第一设备被配置成通过预定加密方法加密流数据和发送加密流数据。 第二发送设备被配置成不经加密流数据地发送流数据。 接收设备被配置成接收从第一发送设备或第二发送设备发送的流数据。接收设备包含接收器和产生器。 接收器被配置成接收从第一发送设备或第二发送设备发送的流数据。产生器被配置成确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。



1.一种发送/接收系统，包括:

第一发送设备，被配置成通过预定加密方法加密流数据并且发送加密的流数据，其中所述流数据被多个公共密钥加密，为该多个公共密钥中的每个分配标识符，并且该多个公共密钥中的每个的所述标识符包含在所述流数据的元数据中;

第二发送设备，被配置成不经加密流数据地发送流数据；和

接收设备，被配置成接收从第一发送设备或第二发送设备发送的流数据;

其中接收设备包含:

接收器，被配置成接收从第一发送设备或第二发送设备发送的流数据，和

产生器，被配置成确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

2.一种用于发送/接收系统的发送/接收方法，包含:

从第一发送设备接收通过预定加密方法加密的流数据或从第二发送设备接收非加密的流数据，并且确定接收的流数据是否被加密，以及

产生指示所获得的确定结果的加密信息，

其中所述流数据被多个公共密钥加密，为该多个公共密钥中的每个分配标识符，并且该多个公共密钥中的每个的所述标识符包含在加密的流数据的元数据中。

3.一种接收在经过第一加密方法的加密之后发送或不经加密地发送的流数据的接收设备，该接收设备包括:

接收器，被配置成接收加密流数据或非加密流数据，其中所述流数据被多个公共密钥加密，为该多个公共密钥中的每个分配标识符，

并且该多个公共密钥中的每个的所述标识符包含在加密的流数据的元数据中；和

产生器，被配置成确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

4.如权利要求3所述的接收设备，还包括：

解密器，被配置成通过第一解密方法对加密流数据执行第一解密过程；和

解密控制器，被配置成当产生器产生的加密信息指示流数据被加密时允许解密器对流数据执行第一解密过程，并且当产生器产生的加密信息指示流数据未被加密时禁止解密器对流数据执行第一解密过程。

5.如权利要求4所述的接收设备，其中第一加密方法和第一解密方法是基于公共密钥的加密方法和解密方法；

用于加密流数据的公共密钥被发送到接收设备；

接收器还接收公共密钥；

当流数据被确定为经过加密时，产生器还向解密器提供被接收器接收的公共密钥；并且

解密器通过使用从产生器提供的公共密钥对流数据执行第一解密过程。

6.如权利要求5所述的接收设备，其中 产生器还在解密器的第一解密过程之前确定公共密钥是否正常，并且产生指示所获得的确定结果的公共密钥准备信息；并且

接收设备还包含呈现器，其根据均由产生器产生的加密信息和公共密钥准备信息来识别接收设备的状态，并且呈现所获得的识别结果。

7.如权利要求6所述的接收设备，其中呈现器

当加密信息指示流数据未被加密时，识别其中接收非加密流数据的第一状态；

当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥正常时，识别第二状态，在该状态中，接收加密流数据并且对流数据正常执行第一解密过程；

当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥不正常时，识别第三状态，在该状态中，接收加密流数据并且对流数据异常执行第一解密过程；以及

呈现第一状态、第二状态或第三状态。

8.如权利要求7所述的接收设备，其中呈现器

包含能够以第一颜色或第二颜色照亮的灯；

使第一状态、第二状态和第三状态与其中灯被禁止以第一颜色或第二颜色照亮的第一灯状态、其中仅允许灯以第一颜色照亮的第二灯状态、或其中仅允许灯以第二颜色照亮的第三灯状态相关；以及

根据情况行使控制以将灯设置在第一灯状态、第二灯状态或第三灯状态，以便呈现第一状态、第二状态或第三状态。

9.如权利要求6所述的接收设备，其中公共密钥在通过第二加密方法进一步加密之后被发送到接收设备，

产生器

当加密公共密钥被接收器接收时，通过与第二加密方法相关的第二解密方法对加密公共密钥执行第二解密过程；

当在解密器的第一解密过程之前成功执行第二解密过程时，向解密器提供公共密钥并且产生指示公共密钥正常的公共密钥准备信息；以及

在其它情况下产生指示公共密钥不正常的公共密钥准备信息。

10.如权利要求9所述的接收设备，其中第二加密方法和第二解密方法是基于公开密钥的公开密钥密码系统，和与公开密钥密码系统相关并且基于私有密钥的解密方法。

11.如权利要求10所述的接收设备，其中 用公开密钥加密的公共密钥被包含在用公共密钥加密的流数据的元数据中，元数据被叠加在流数据上，并且在其上叠加有元数据的流数据被发送到接收设备；

产生器

当元数据被叠加在接收设备接收的流数据上时，产生指示流数据被加密的加密信息，从元数据中提取加密的公共密钥，并且对公共密钥执行使用对应于公开密钥的私有密钥的第二解密过程；并且

当元数据未被叠加在接收设备接收的流数据上时，产生指示流数据未被加密的加密信息。

12.如权利要求11所述的接收设备，其中不同于特殊值的标识符被分配给该多个公共密钥中的每个；并且

当在元数据被叠加在接收设备接收的流数据上的情况下元数据中包含的标识符是该特殊值时，产生器禁止生成指示流数据被加密的加密信息，并且产生指示流数据未被加密的加密信息。

13.如权利要求6所述的接收设备，还包括： 再现控制器，当解密控制器允许执行第一解密过程时，再现控制器控制当解密器对加密流数据执行第一解密过程时获得的第一流数据的再现；并且当解密控制器禁止执行第一解密过程时，控制被接收器接收并且未加密的第二流数据的再现。

14.如权利要求13所述的接收设备，其中 当在解密控制器允许执行第一解密过程的情况下公共密钥准备信息指示公共密钥不正常时，再现控制器禁止再现第一流数据，但是控制根据预定规则产生的数据

的再现。

15.如权利要求14所述的接收设备，其中，其再现由再现控制器控制的、代替第一流数据的数据是对应于预定固定图像的图像数据。

16.如权利要求14所述的接收设备，其中，其再现由再现控制器控制的、代替第一流数据的数据是这样的图像数据，该图像数据对应于其再现在该数据的再现控制之前得到控制的第一流数据中的预定静止图片。

17.如权利要求5所述的接收设备，其中 加密流数据经由第一路径被发送到接收设备，并且由加密流数据使用的公共密钥经由第二路径被发送到接收设备；并且

接收器包含

第一接收器，其接收经由第一路径发送的非加密流数据或加密流数据，和

第二接收器，其接收经由第二路径发送的公共密钥。

18.一种用于接收设备的接收方法，该接收设备接收在通过预定加密方法加密之后发送的流数据，或不经加密地发送的流数据，

该接收方法包括步骤：

确定接收设备接收的流数据是否被加密和产生指示所获得的确定结果的加密信息，

其中在被加密之后发送的所述流数据被多个公共密钥加密，为该多个公共密钥中的每个分配标识符，并且该多个公共密钥中的每个的所述标识符包含在加密的流数据的元数据中。

发送/接收系统、发送/接收方法、接收设备、接收方法和程序

对相关专利申请的交叉引用

本发明包含于与 2006年 8月 16日向日本专利局提交的日本专利申请 JP 2005- 235639有关的主题，这里参考引用了该专利申请的全部内容。

技术领域

本发明涉及发送/接收系统、发送/接收方法、接收设备、接收方法和程序，尤其涉及允许接收端容易地处理从发送端发送的数字资料(无论其是否加密)以便再现的发送/接收系统、发送/接收方法、接收设备、接收方法和程序。

背景技术

近年来，用于数字资料 (内容)的发送/接收系统已经得到广泛使用 (例如参照日本专利应用 JP 2003 - 143548)。此外，存在用于在影院播放数字资料的计划，并且正在研究和开发用于这样的计划的发送/接收系统。

构成这样的发送/接收系统的单元 (未示出)将是例如第一服务器、第二服务器、路由器和投影仪。第一服务器加密和发送电影的流数据。 路由器选择和发送从第一或第二服务器发送的数据 (输出信号)。投影仪接收从路由器发送的数据并且播放涉及所接收数据的电影、预告片或广告。

发明内容

在包含上述单元的发送/接收系统，即包含第一服务器、第二服务器、路由器和投影仪的发送/接收系统中，投影仪可以接收加密流数据和非加密流数据。然而，尚未得到用于允许投影仪以区别对待的方式处理这样的流数据的适当方法。

本发明解决了上述问题，并且无论其是否被加密，均允许接收端容易地处理从发送端传送的数字资料以进行数字资料再现。

根据本发明的一个实施例，发送/接收系统包含：第一发送设备，被配置成通过预定加密方法加密流数据并且发送加密的流数据；第二发送设备，被配置成发送没有加密的流数据；和接收设备，被配置成接收从第一发送设备或第二发送设备发送的流数据。接收设备包含：接收器，被配置成接收从第一发送设备或第二发送设备发送的流数据， 和产生器，被配置成确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

根据本发明的另一实施例，用于发送/接收系统的发送/接收方法包含第一发送设备，被配置成通过预定加密方法加密流数据和发送加密的流数据，第二发送设备，被配置成发送非加密的流数据，和接收设备，被配置成接收从第一发送设备或第二发送设备发送的流数据。接收设备确定接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

根据本发明实施例的发送/接收系统和发送/接收方法被应用于发送/接收系统。发送/接收系统包含第一发送设备，被配置成通过预定加密方法加密流数据和发送加密的流数据，第二发送设备，被配置成发送非加密的流数据，和接收设备，被配置成接收从第一发送设备或第二发送设备发送的流数据。发送/接收系统内的接收设备确定接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

根据本发明的另一实施例，接收设备接收通过第一加密方法加密的流数据，或接收发送到该设备的非加密流数据。接收设备包含：接收器，被配置成接收加密流数据或非加密流数据；和产生器，被配置成确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息。

接收设备还可以包含解密器和解密控制器。解密器被配置成通过第一解密方法对加密流数据执行第一解密过程。解密控制器被配置成当产生器产生的加密信息指示流数据被加密时允许解密器对流数据

执行第一解密过程。解密控制器被配置成当产生器产生的加密信息指示流数据未被加密时禁止解密器对流数据执行第一解密过程。第一加密方法和第一解密方法可以是基于公共密钥的加密方法和解密方法。用于加密流数据的公共密钥可以被发送到接收设备。接收器还可以接收公共密钥。当流数据被确定为经过加密时，产生器还可以提供被接收器接收的公共密钥。解密器可以通过使用从产生器提供的公共密钥对流数据执行第一解密过程。

产生器还可以在解密器的第一解密过程之前确定是否正常准备公共密钥，并且产生指示所获得的确定结果的公共密钥准备信息。接收设备还可以包含指示器，其根据均由产生器产生的加密信息和公共密钥准备信息识别接收设备的状态，并且呈现所获得的识别结果。

指示器可以识别和呈现第一状态、第二状态和第三状态。第一状态是当加密信息指示流数据未被加密时的状态，其中接收非加密流数据。第二状态是当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥被正常准备时的状态，其中接收加密流数据并且对流数据正常执行第一解密过程。第三状态是当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥未被正常准备时的状态，其中接收加密流数据但是对流数据异常执行第一解密过程。

指示器可以包含能够以第一颜色或第二颜色照亮的灯。指示器使第一状态、第二状态和第三状态与其中灯被禁止以第一颜色或第二颜色照亮的第一灯状态、其中仅允许灯以第一颜色照亮的第二灯状态、或其中仅允许灯以第二颜色照亮的第三灯状态相关。指示器根据情况行使控制以将灯设置在第一灯状态、第二灯状态或第三灯状态，以便呈现第一状态、第二状态或第三状态。

在经过第二加密方法的进一步加密之后，公共密钥可以被发送到接收设备。当加密公共密钥被接收器接收时，产生器可以通过与第二加密方法相关的第二解密方法对加密公共密钥执行第二解密过程。当在解密器的第一解密过程之前成功执行第二解密过程时，产生器可以向解密器提供公共密钥并且产生指示公共密钥被正常准备的公共密

钥准备信息。产生器可以在其它情况下产生指示公共密钥未被正常准备的公共密钥准备信息。

第二加密方法和第二解密方法可以是基于公开密钥的公开密钥密码系统，和与公开密钥密码系统相关并且基于私有密钥的解密方法。

经过公开密钥加密的公共密钥可以被包含在经过公共密钥加密的流数据的元数据中。元数据可以被叠加在流数据上，并且其上叠加有元数据的流数据可以被发送到接收设备。当元数据被叠加在接收设备接收的流数据上时，产生器可以产生指示流数据被加密的加密信息，从元数据中提取加密公共密钥，并且对公共密钥执行使用对应于公开密钥的私有密钥的第二解密过程。当元数据未被叠加在接收设备接收的流数据上时，产生器可以产生指示流数据未被加密的加密信息。

流数据可以使用多个公共密钥。不同于特殊值的标识符可以被分配给该多个公共密钥中的每个。该多个公共密钥中的每个的标识符可以被包含在元数据中。当在元数据被叠加在接收设备接收的流数据上的情况下元数据中包含的标识符是该特殊值时，产生器可以禁止生成指示流数据被加密的加密信息，并且产生指示流数据未被加密的加密信息。

接收设备还可以包含再现控制器，当解密控制器允许执行第一解密过程时，再现控制器控制当解密器对加密流数据执行第一解密过程时获得的第一流数据的再现。当解密控制器禁止执行第一解密过程时，再现控制器控制被接收器接收并且未加密的第二流数据的再现。

当在解密控制器允许执行第一解密过程的情况下公共密钥准备信息指示公共密钥未被正常准备时，再现控制器可以禁止再现第一流数据，但是控制根据预定规则产生的数据的再现。当公共密钥准备信息指示公共密钥被正常准备时，再现控制器可以控制第一流数据的再现。

其再现由再现控制器控制的数据而不是第一流数据可以是对应

于预定固定图像的图像数据。

其再现由再现控制器控制的数据而不是第一流数据可以是这样的图像数据，该图像数据对应于其再现在该数据的再现控制之前得到控制的第一流数据中的预定静止图片。

加密流数据可以经由第一路径被发送到接收设备，并且由加密流数据使用的公共密钥可以经由第二路径被发送到接收设备。接收器可以包含接收经由第一路径发送的非加密流数据或加密流数据的第一接收器，和接收经由第二路径发送的公共密钥的第二接收器。

根据本发明的另一实施例，接收方法/程序将由计算机来执行，该计算机用于控制接收设备的接收方法/硬件，该接收设备接收在通过预定加密方法加密之后发送的流数据或不经加密地进行发送的流数据。该接收方法/程序包含确定接收设备接收的流数据是否被加密和产生指示所获得的确定结果的加密信息的步骤。

根据本发明实施例的接收设备、接收方法和程序适用于这样的接收设备/硬件，其接收在通过预定加密方法加密之后发送的流数据，或不经加密地进行发送的流数据。该接收方法/硬件确定接收的流数据是否被加密并且产生指示所获得的确定结果的加密信息。

如上所述，本发明的实施例使得能够接收非加密流数据以及加密流数据。

尤其是当要播放构成数字资料的流数据时，接收端能够容易地确定从发送端发送的数字资料是否被加密。因此，接收端能够容易地处理数字资料，无论其是否被加密。

附图说明

图1的模块图图解了根据本发明实施例的发送/接收系统的典型配置；

图2的模块图图解了图1示出的发送/接收系统中的电影院服务器的典型配置；

图3图解了由图2示出的电影院服务器产生的元数据在 AV数据上叠加的典型位置；

图4示出了元数据的典型结构，元数据包含用于图4示出的电影院服务器中的加密以及图1示出的投影仪中的解密的数据；

图5示出了元数据的典型结构，元数据包含用于图4示出的电影院服务器中的加密以及图1示出的投影仪中的解密的数据；

图6示出了元数据的典型结构，元数据包含用于图4示出的电影院服务器中的加密以及图1示出的投影仪中的解密的数据；

图7的模块图图解了图1示出的发送/接收系统中的子AV服务器的典型配置；

图8的模块图图解了图1示出的发送/接收系统中的投影仪的典型配置；

图9的模块图图解了图8示出的投影仪中元数据提取部分的典型配置的细节；

图10的流程图图解了由图8示出的投影仪执行的典型过程；

图11的模块图图解了根据本发明实施例的发送/接收系统的另一典型配置，其不同于图1示出的配置；

图12的模块图图解了图11示出的发送/接收系统中电影院服务器的典型配置，其不同于图2示出的配置；

图13的模块图图解了图11示出的发送/接收系统中投影仪的典型配置，其不同于图8示出的配置；

图14的模块图图解了图11示出的投影仪中元数据提取部分的典型配置的细节，该典型配置不同于图9示出的配置；而

图15的模块图图解了执行根据本发明实施例的程序的个人计算机的典型配置。

具体实施方式

现在描述本发明的实施例。下面示例说明本发明的组成特征与具体实施方式部分中描述的实施例之间的关系。此声明表明支持本发明的实施例是在具体实施方式部分中描述的。 因此，虽然在具体实施方式部分描述了各实施例，然而即使某个实施例这里未被描述为对应于本发明的组成特征的实施例，也不意味着该实施例不对应于该组成

特征。相反，即使实施例在这里描述为对应于该组成特征的实施例，也不意味着该实施例不对应于其它组成特征。

根据本发明实施例的发送/接收系统 (例如图1或图11示出的发送/接收系统；然而，以下描述仅仅涉及图1示出的发送/接收系统)包含第一发送设备、第二发送设备和接收设备。 第一发送设备 (例如图1示出的电影院服务器 1)通过预定加密方法加密流数据，并且发送加密流数据。第二发送设备 (例如图1示出的子AV服务器 2）不经加密地发送流数据。接收设备 (例如图1示出的并且如图8所示配置的投影仪 4)接收从第一或第二发送设备发送的流数据。接收设备包含接收器(例如图8示出的接收器部分 71)和产生器 (例如图8示出的元数据提取部分 72)。接收器接收从第一或第二发送设备发送的流数据。产生器确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息 (例如图8示出的加密输入信号 102)。

根据本发明实施例的发送/接收系统是用于上述根据本发明实施例的发送/接收系统的接收方法。接收设备 (例如图1示出的并且如图8所示配置的投影仪 4)包含确定接收的流数据是否被加密并且产生指示所获得的确定结果的加密信息的步骤 (例如图10示出的步骤 S2)。

根据本发明实施例的接收设备 (例如图1示出的并且如图8所示配置的投影仪 4，或图11示出的并且如图13所示配置的投影仪 202；然而，除了在只支持投影仪 202的情况下，以下描述涉及投影仪 4）接收流数据， 在通过第一加密方法加密之后发送流数据 (例如从图1示出的电影院服务器 1发送的加密 AV数据)，或不经加密地发送流数据 (例如从图1示出的子AV服务器 2发送的非加密 AV数据)。接收设备包含接收器(例如图8示出的接收器部分 71)和产生器 (例如图8示出的元数据提取部分 72)。接收器接收加密或非加密流数据。产生器确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息 (例如图8示出的加密输入信号 102)。

接收设备还包含解密器 (例如图8示出的解密部分 73)和解密控制器 (例如图8示出的切换部分 75)。解密器通过对应于第一加密方法

的第一解密方法对加密流数据执行第一解密过程。解密控制器当产生器产生的加密信息指示流数据被加密时允许解密器对流数据执行第一解密过程，并且当产生器产生的加密信息指示流数据未被加密时禁止解密器对流数据执行第一解密过程。

第一加密方法和第一解密方法是基于公共密钥 (例如图8示出的LE密钥31-D)的加密方法和解密方法。用于加密流数据的公共密钥可以被发送到接收设备。接收器还接收公共密钥。当流数据被确定为要经过加密时，产生器还向解密器提供被接收器接收的公共密钥。解密器通过使用从产生器提供的公共密钥对流数据执行第一解密过程。

产生器还在解密器的第一解密过程之前确定是否正常准备公共密钥，并且产生指示所获得的确定结果的公共密钥准备信息 (例如图8示出的密钥未发现信号 101)。接收设备还包含呈现器 (例如图8示出的状态呈现部分 74），其根据均由产生器产生的加密信息和公共密钥准备信息来识别接收设备的状态，并且呈现所获得的识别结果。

呈现器识别并且呈现第一状态 (例如在图10示出的步骤 S8提及的"非加密输入状态")、第二状态 (例如在图10示出的步骤 S6提及的"加密输入正常状态")、或第三状态 (例如在图10示出的步骤 S10提及的"加密输入差错状态")。第一状态是当加密信息指示流数据未被加密时的状态，其中接收非加密流数据。第二状态是当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥被正常准备时的状态，其中接收加密流数据并且对流数据正常执行第一解密过程。第三状态是当加密信息指示流数据被加密并且公共密钥准备信息指示公共密钥未被正常准备时的状态，其中接收加密流数据但是对流数据异常执行第一解密过程。

在经过第二加密方法的进一步加密之后，公共密钥可以被发送到接收设备。当加密公共密钥被接收器接收时，产生器通过与第二加密方法相关的第二解密方法对加密公共密钥执行第二解密过程 (例如图9示出的 LEKP恢复部分执行相关过程)。当在解密器的第一解密过程之前成功执行第二解密过程时，产生器向解密器提供公共密钥 (例如

图9示出的寄存器125执行相关过程)，并且产生指示公共密钥正常准备的公共密钥准备信息 (例如图9示出的 LEKP表 123执行相关过程)。产生器在其它情况下产生指示公共密钥未被正常准备的公共密钥准备信息 (例如图9示出的 LEKP表 123执行相关过程)。

第二加密方法和第二解密方法是基于公开密钥的公开密钥密码系统 (此后描述的 RSA加密方法)，和与公开密钥密码系统相关并且基于私有密钥的解密方法。

用公开密钥加密的公共密钥被包含在用公共密钥加密的流数据的元数据 (例如图8示出的元数据34; 更具体地，图4示出的元数据34-1或图5示出的元数据34-2，其被包含为 Elekp数据)中。 元数据被叠加在流数据上，并且其上叠加有元数据的流数据被发送到接收设备。当元数据被叠加在接收设备接收的流数据上时，产生器产生指示流数据被加密的加密信息，从元数据中提取加密公共密钥，并且对公共密钥执行使用对应于公开密钥的私有密钥的第二解密过程。当元数据未被叠加在接收设备接收的流数据上时，产生器产生指示流数据未被加密的加密信息。

流数据使用多个公共密钥。不同于特殊值 (例如以后例子中的 0)的标识符被分配给多个公共密钥中的每个。该多个公共密钥中的每个的标识符可以被包含在元数据中。

当在元数据被叠加在接收设备接收的流数据上的情况下元数据中包含的标识符是该特殊值时，产生器禁止生成指示流数据被加密的加密信息，并且产生指示流数据未被加密的加密信息 (例如图9示出的元数据提取/分离部分 121执行相关过程)。

接收设备还包含再现控制器 (例如图8示出的切换部分 79和再现控制部分 80)。当解密控制器允许执行第一解密过程时，再现控制器控制当解密器对加密流数据执行第一解密过程时获得的第一流数据的再现。当解密控制器禁止执行第一解密过程时，再现控制器控制被接收器接收并且未加密的第二流数据的再现。

当在解密控制器允许执行第一解密过程的情况下公共密钥准备

信息指示公共密钥未被正常准备时，再现控制器禁止再现第一流数据，但是控制根据预定规则产生的数据的再现 (例如改变切换部分 79的输入以选择切换部分 78)。

其再现由再现控制器控制的数据而不是第一流数据是对应于预定固定图像的图像数据 (例如图8示出的固定图像存储部分 76中存储的固定图像数据)。其再现由再现控制器控制的数据而不是第一流数据是这样的图像数据 (例如图8示出的帧存储部分 77中存储的帧数据)，该图像数据对应于其再现在该数据的再现控制之前得到控制的第一流数据中的预定静止图片。

对于接收设备 (这里，假定接收设备是图11的例子中示出的投影仪 202)，加密流数据 (例如从图11示出的电影院服务器 201发送的加密 AV数据)经由第一路径 (例如经由图11示出的路由器 3的路径)被发送到接收设备。加密流数据使用的公共密钥 (例如图11示出的 LE密钥+密钥ID 211)经由第二路径 (例如经由网络 203的路径)被发送到接收设备。接收器包含接收经由第一路径发送的非加密流数据或加密流数据的第一接收器 (例如图13示出的 AV接收器部分 231)，和接收经由第二路径发送的公共密钥的第二接收器 (例如图13示出的密钥接收器部分 232)。

根据本发明实施例的接收方法/程序与上述根据本发明实施例的接收设备 (例如图1示出的并且如图8所示配置的投影仪 4)相关。该接收方法/程序包含确定接收的流数据是否被加密和产生指示所获得的确定结果的加密信息的步骤 (图10示出的步骤 S2)。

现在参考附图详细描述本发明的实施例。图1图解了根据本发明实施例的发送/接收系统的典型配置。

图1示出的发送/接收系统被用于在电影院等等中播放由数字资料组成的内容。根据本发明实施例的再现内容包含作为主要内容片段的电影和作为附带内容片段的预告片和广告。因此，图1示出的发送/接收系统包含电影院服务器1、子AV服务器2、路由器3和投影仪4。

由于系统可以包含某些附加设备，所以使用词语"包含"。这对

于后续描述同样适用。

在图1示出的例子中，电影院服务器1以例如 HD-SDI信号的形式输出作为主要内容数据的电影的流数据。在这种情况下，电影院服务器1使用作为各种基于公共密钥的加密方法 (此后被称作公共密钥密码系统)之一的 AES (先进加密标准)来加密和输出流数据，以保护主要内容。

其间，子AV服务器2以例如 HD-SDI信号的形式输出作为附带内容数据的预告片和广告的流数据。从子AV服务器2输出的流数据未被加密。

从电影院服务器1输出的流数据 (HD-SDI输出信号)此后被称作加密AV数据。从子AV服务器2输出的流数据 (HD-SDI输出信号)此后被称作非加密AV数据。在电影院服务器1内仍然未加密的流数据 (图2示出并且以后描述的 AV数据存储部分11中存储的流数据)，加密AV数据 (从电影院服务器1输出的流数据）和非加密AV数据 (从子AV服务器2输出的流数据)被共同称作 AV数据。

路由器3选择来自电影院服务器1的加密AV数据或来自子AV服务器2的非加密AV数据，并且提供选择的 AV数据到投影仪4。

投影仪4从路由器3接收 AV数据并且控制对应于接收的 AV数据的内容的再现。更具体地，投影仪4处理电影、预告片和广告的视频和音频，在屏幕等等上投射视频，并且从扬声器等等输出音频。

下面将按照所列顺序详细描述图1示出的发送/接收系统的电影院服务器1、子AV服务器2和投影仪4。

图2图解了电影院服务器1的典型配置。

在图2中，实线方块表示设备或系统 (在当前例子中为电影院服务器1)的模块或组成部分，虚线方块表示预定信息项。实线和虚线的这种选择性使用也适用于后续描述中引用的其它附图。

在图2示出的例子中，电影院服务器1包含 AV数据存储部分11、加密部分12、元数据产生部分13、叠加部分14和发送器部分15。

AV数据存储部分11存储对应于电影的一或多个 AV数据。

在图2示出的例子中，加密部分12包含 AES加密数据产生部分21和 AV数据加密部分22。

AES加密数据产生部分21使用作为用于 AES的公共密钥的 LE密钥31-E (可以被称为 AES密钥)和 AES输入32-E来产生用于直接加密 AV数据存储部分11中存储的预定 AV数据的数据35 (此后被称作AES加密数据35)，并且提供产生的数据到 AV数据加密部分22。 后面会描述 AES输入32-E。

AV数据加密部分22使用从 AES加密数据产生部分21输送的AES加密数据35加密 AV数据存储部分11中存储的一或多个 AV数据段中的预定数据段，并且提供所得到的加密 AV数据到叠加部分14。在这种情况下， AV数据加密部分22使用从元数据产生部分13输送的帧复位33-E以帧为单位加密 AV数据。

出于说明的目的，假定根据本发明实施例的 AV数据是如上所述的 HD-SID信号，并且由一或多个帧数据段组成。也假定帧数据包含指示构成该帧的所有像素的亮度的数据Y，和指示构成该帧的所有像素的颜色的数据Cb/Cr。此外，假定 LE密钥31-E和 AES输入32-E由128位组成。

在上述情况下， AES加密数据产生部分21例如由具有 128位LE密钥31-E和 128位 AES输入32-E的 256位输入数据产生 128位AES加密数据35，并且提供产生的数据到 AV数据加密部分22。 更具体地， AES加密数据产生部分21例如以 10位为单位获得 128位AES加密数据35的低 120位以作为实际用于 AV数据加密的数据，并且提供获得的位到 AV数据加密部分22。

AV数据加密部分22逐个地使用每组 10位数据，实时转换数据Y和数据Cb/Cr，并且提供加密数据到叠加部分14。

然而在下面的说明中，除了在需要彼此区分它们时，数据Y和数据Cb/Cr通常被称作 AV数据。

元数据产生部分13产生加密部分12的加密处理所需的各种信息项 (即用于后面会描述的投影仪 (投影仪4)的解密过程的各种信息

项)，例如 LE密钥31-E、 AES输入32-E和帧复位33-E。此外，通过向 LE密钥31-E增加一些上述各种信息项以作为补充信息，元数据产生部分13产生称作 LEKP (链接加密密钥有效负载)的数据。接着，元数据产生部分13通过使用投影仪4的公开密钥的加密方法 (此后被称作公开密钥密码系统)，更具体地，通过例如 RSA (R. Rivest 、 A. RSA 、 L. Adelman) (商标) 2048位加密方法 (此后被称作 RSA加密方法)，对 LEKP执行加密处理。当通过 RSA加密方法加密 LEKP时获得的数据此后被称作 ELEKP 。换言之,元数据产生部分13产生ELEKP。除了 ELEKP之外,元数据产生部分13产生包含 AES输入32-E的单元 (后面会描述的 Le_attribute_data （LE属性数据）)，并且提供产生的元数据到叠加部分14。 后面会参照图4到 6描述元数据34的例子。

叠加部分14在从 AV数据加密部分22发送的加密AV数据的预定部分上叠加从元数据产生部分13发送的元数据34。 从叠加部分14向发送器部分15提供其上叠加有元数据34的加密AV数据。

更具体地，如图3所示，在其 V-ANC (V空白时段)期间，本实施例在构成加密AV数据的每个帧数据 (一个帧)上叠加一个元数据34。

图3的左半部指示在逐行（progressive）(P)的情况下元数据34的插入 (叠加)位置，右半部指示在逐行分割帧 (P)或隔行(interlace）(I)的情况下元数据34的插入 (叠加)位置。术语"H-ANC"表示 H空白区。术语"活动视频区"表示所谓的有效线区。

返回图2，发送器部分15以帧为单位向图1示出的路由器3发送从叠加部分14输送的加密AV数据，即在其上叠加有元数据34的加密AV数据。本实施例不针对一段 AV数据 (全部流数据)使用一个 LE密钥31-E。可以执行更新。换言之，多个 LE密钥31-E被用于一段 AV数据。原因如下。

如果恶意第三方在用一种 AES密钥 (当前例子中的 LE密钥31-E)加密内容的情况下窃用 AES加密内容 (当前例子中电影的

AES加密AV数据)，则会增加 AES密钥被直接解密的危险。为解决这个问题，根据本实施例的元数据产生部分13周期性改变 AES密钥 (更新 AES密钥)，以便使得第三方难以直接解密内容。在本实施例中，电影院服务器1通过不直接原样发送 LE密钥31-E来保护 LE密钥31-E。更具体地，如上所述，元数据产生部分13产生作为 LE密钥31-E和补充数据的组合的 LEKP，对 LEKP执行 RSA加密处理，并且产生包含所得到的 ELEKP的元数据34。叠加部分14接着在加密AV数据上叠加元数据34。发送器部分15发送在其上叠加有元数据34的加密AV数据。

换言之，根据本实施例的电影院服务器1对多个 LE密钥31-E中的每个执行 RSA加密过程，并且经由路由器3向投影仪4发送该多个RSA加密的 LE密钥31-E中的每个 (在按照产生顺序被包含在预定帧中之后)。 因此，如下所述，投影仪4也对该多个 RSA加密的 LE密钥31-E中的每个执行 RSA解密过程。

如上所述，对于对应于电影的 AV数据，本实施例使用多个 LE密钥31-E而不是只使用一个 LE密钥31-E (可以执行更新)。更具体地，用于加密构成 AV数据段的每个帧 (数据)的 LE密钥31-E不局限于一个。更新 LE密钥31-E以便对每批某个数目的帧使用新 LE密钥31-E。

因此，在本实施例中，每当产生该多个 LE密钥31-E时，元数据产生部分13将 LE密钥标识符 (此后被称作密钥 ID)附加到该多个LE密钥31-E中的每个上。如下所述，密钥ID也被包含在元数据34中。然而，预定特殊值 (本实施例中的值 0)未被作为密钥ID来附加 (被排除)。

需要在 AV数据加密部分22对 AV数据执行加密过程之前产生用于 AV数据加密的 LE密钥31-E。换言之，在产生加密AV数据的时刻和产生用于 AV数据加密的 LE密钥31-E的时刻之间存在时滞。结果，在叠加部分14中，当加密AV数据的预定帧 (数据)被加密时不使用该预定帧 (数据)上叠加的元数据34中包含的 LE密钥31-E (更准确

地说， RSA加密之前的 LEKP中包含的 LE密钥31-E)，并且该 LE密钥31-E将被用于加密在预定帧之后到达的帧 (数据)。

在详细描述子AV服务器2和投影仪4 (图1)的例子之前将参照图4描述由元数据产生部分13产生的元数据34的例子。

图4和 5示出了包含上述 ELEKP (RSA加密的 LE密钥31-E等等)的元数据34-1和 34-2的典型结构。图6示出了包含 AES输入32-E的元数据34 - 3的典型结构。

本实施例使用的元数据34-1、 34-2和 34-3的分组结构遵照 SMPTE (动画和电视工程师协会） 291M标准 (针对电视辅助数据分组和间隔格式的建议 SMPTE标准)。它们通常分别被称作元分组 1、2和 3。在由 SMPTE 291M标准定义的分组结构中，如图4到 6所示，包含 ADF (辅助数据标记 (000、 3FF、用于分量的 3FF; 用于复合的 3FC))、 DID (数据ID)、 SDID (辅助数据ID)、 DC (数据计数)、用户数据和 CS (校验和)按照所列的顺序排列。 元数据34-1、 34-2和 34-3具有这样的分组结构。在本实施例中，用户数据包含以下信息项。

在元数据34-1内，用户数据包含密钥ID、类型、 SHAI摘要、Lekp长度、 Elekp长度和 Elekp数据。元数据34-2内的用户数据包含Elekp数据。

下面将按随机顺序提供说明。如前所述， Elekp数据是 ELEKP，即当对包含 LE密钥31-E等等的 LEKP执行 RSA加密过程时获得的数据。如前所述，密钥ID是被加密并且包含在 ELEKP中的 LE密钥31-E的标识符。Elekp长度是 ELEKP的数据长度。Lekp长度是对应于 ELEKP的 LEKP的数据长度。

类型是用于 LEKP加密的加密方法 (算法类型)。在本实施例中，表示 RSA加密方法的值 0被替代入该类型。SHAI摘要是当产生ELEKP时 (当对 LEKP进行 RSA加密时)使用的公开密钥的标识符。

包含上述各种信息项的元数据34-1和元数据34-2中的用户数据此后被称作 LEKM (链接加密密钥消息)。

不同于以上 LEKM (元数据34-1和元数据34-2中的用户数据)，元数据34-3中的用户数据包含下一密钥ID、当前密钥ID、当前帧计数、密钥改变定时和 HD-SDI链路数。

目标元数据34-3所插入到的帧，更准确地说，元数据34-3所插入到的 AV数据帧数据被称为相关帧。此外，例如紧接在相关帧的加密开始之前的 LE密钥32-E被称为当前 LE密钥32-E。要接着当前 LE密钥32-E产生的 LE密钥32-E (要在下一更新时间由元数据产生部分13产生）被称为下一 LE密钥32-E。紧接在当前 LE密钥32-E 之前产生的 LE密钥32-E(由元数据产生部分13在前面更新时间产生)被称为前面的 LE密钥32-E。

插入到相关帧中的元数据34-3中的下一密钥ID、当前密钥ID、当前帧计数、密钥改变定时和 HD-SDI链路数是如下所述的信息。

下一密钥ID是下一 LE密钥32-E的密钥ID。当前密钥ID是当前LE密钥32-E的密钥ID。

当前帧计数是指示当从某帧（0号帧）执行计数时哪个编号的帧是相关帧，该某帧是当前面的 LE密钥32-E被更新为当前 LE密钥32-E时的帧 (此时刻此后被称作密钥改变定时)。

2'b11、2'b10、2'b01或2'b00被替代入密钥改变定时。这些值指示下一密钥改变定时表示什么帧。例如，值 2'b11 (＝3)指示密钥改变定时表示从相关帧开始的第三或后续帧。值2'b10 (＝2)指示该密钥改变定时表示从相关帧开始的第二帧。值 2'b01 (＝1)指示该密钥改变定时表示从相关帧开始的第一帧 (即下一帧)。值2'b00 (＝0)指示该密钥改变定时表示相关帧。

HD-SDI链路数是指示电影院服务器1和投影仪4之间 HD-SDI信号传输的类型 (本实施例中的加密AV数据传输类型)的值。例如当值0被替代为 HD-SDI链路数时，它指示链路-A，链接-A是单个链路 (基于一个 HD-SDI接口的传输类型)或双链路 (基于 2个 HD-SDI接口的传输类型)。例如当值 1被替代为 HD-SDI链路数时，它指示作为双链路的链路 - B。

插入到相关帧中的元数据34-1、34-2的 ELEKP中包含的 LE密钥31-E (更准确地说，是非加密 LEKP中包含的)被用于加密位于相关帧之后的帧。换言之，用于相关帧的 LE密钥31-E被包含在插入到相关帧前面的帧中的元数据34-1、 34-2的 ELEKP中 (更准确地说，是包含在非加密 LEKP中)。

在本实施例中，如上所述，在其上叠加有元数据34-1到 34-3的加密AV数据由电影院服务器1 (图1和 2)来产生，并且可以经由路由器3被发送到投影仪4。

现在将参照图7详细描述图1示出的子AV服务器2。图7图解了子AV服务器2的典型配置。在图7示出的例子中，子AV服务器2包含 AV数据存储部分 51和发送器部分 52。

AV数据存储部分 51存储对应于电影预告片和广告的一或多个AV数据段。

发送器部分 52向图1示出的路由器3发送一段非加密 AV数据，即 AV数据存储部分 51中存储的一或多个 AV数据段中的预定一段。 现在将参照图8到 10详细描述图1示出的投影仪4。

图8图解了投影仪4的典型配置。 在图8示出的例子中，投影仪4包含接收器部分 71，元数据提取部分 72，解密部分 73，状态呈现部分 74，切换部分 75、 78、 79，固定图像存储部分 76，帧存储部分 77和再现控制部分 80。

接收器部分 71从路由器3 (图1)接收 AV数据。 更具体地，接收器部分 71从电影院服务器1 (图1和 2)接收加密 AV数据，或从子AV服务器2 (图1 和 7)接收非加密 AV数据。

元数据提取部分 72确定由接收器部分 71接收的 AV数据是加密的还是非加密的。

当所获得的确定结果指示 AV数据被加密时，元数据提取部分72产生加密检测信号 102 (根据图8，此后被称作加密输入信号 102)并且将其提供给状态呈现部分 74和切换部分 75。 此外，元数据提取部分 72从加密AV数据中提取元数据34 (本实施例中的元数据34-1

到 34-3)和其它信息。元数据提取部分 72接着由提取的信息产生 LE密钥31-D、 AES输入32-D和帧复位33-D，并且将其提供给解密部分73。分别从当电影院服务器1产生加密 AV数据时使用的LE密钥31-E、AES输入32-E和帧复位33-E中恢复出 LE密钥31-D、 AES输入32-D和帧复位33-D。因此，能够理解，元数据提取部分 72恢复出 LE密钥31-E、 AES输入32-E和帧复位33-E并且将其提供给解密部分 73。

如果出于某种原因没有正常产生 LE密钥31-D (没有恢复 LE密钥31-E)，即如果没有针对以后描述的解密部分 73寄存 (未提供)作为解密密钥的 LE密钥31-D，则元数据提取部分72产生解密密钥未寄存信号101 (根据图8，此后被称作密钥未发现信号101)并且将其提供给状态呈现部分74、帧存储部分77和切换部分79。

另一方面，当接收器部分 71接收非加密 AV数据时，非加密AV数据不包含元数据34，使得元数据提取部分 72不能提取元数据34。当元数据34未被叠加在由接收器部分 71接收的 AV数据上时，元数据提取部分 72确定 AV数据没有加密，并且禁止产生加密输入信号102。

当在其上叠加有元数据34的 AV数据被接收器部分 71接收的情况下满足预定条件时， AV数据可以被认为是非加密 AV数据，从而禁止产生加密输入信号 102。后面会描述上述预定条件。

可以假定密钥未发现信号 101的水平为 Hi(1)或 Lo(0)。Hi水平("1"水平)可以被认为是产生密钥未发现信号 101。Lo水平 ("0"水平)可以被认为是禁止密钥未发现信号 101产生。当LE密钥31-D被正常产生 (恢复 LE密钥31-E)时，在这种情况下，密钥未发现信号 101的水平为 Lo(0)。

当LE密钥31-D未被正常产生 (未恢复 LE密钥31-E)时，密钥未发现信号 101的水平为 Hi(1)。

类似地，也可以假定加密输入信号 102的水平为 Hi(1)或Lo(0)。Hi水平 ("1"水平)可以被认为是产生加密输入信号 102。Lo水平 ("0"水平)可以被认为是禁止加密输入信号 102产生。当加密

AV数据被接收器部分 71接收时，在这种情况下，加密输入信号 102的水平为 Hi(1)。当非加密 AV数据被接收器部分 71接收时，加密输入信号 102的水平为 Lo(0)。

以下说明假定密钥未发现信号 101和加密输入信号 102的水平为 Hi(1)或 Lo(0)。

上面已经概述了元数据提取部分 72。下面参照图9详细描述元数据提取部分 72。

在图8示出的例子中，解密部分 73包含 AES解密数据产生部分 91和 AV数据解密部分 92。

AES解密数据产生部分 91使用从元数据提取部分 72提供的 LE密钥31-D和 AES输入32-D产生用于直接对加密 AV数据进行解密的数据 103 (此后被称作 AES解密数据 103)，并且将其提供给 AV数据解密部分 92。 换言之， AES解密数据 103是对应于图2示出的 AES加密数据35的解密数据。

AV数据解密部分 92使用从 AES解密数据产生部分 91提供的 AES解密数据 103对接收器部分 71接收的加密AV数据执行解密过程，并且提供所得到的 AV数据 (此后被称作恢复的 AV数据，以便区别于非加密 AV数据)给切换部分 75。 在这种情况下， AV数据解密部分 92使用从元数据提取部分 72提供的帧复位33-D以帧为单位解密加密AV数据。

应当指出，在这种情况下，相同 AES解密数据 103未被用于作为流数据的整个加密 AV数据。如前所述，使用对应于由电影院服务器1以预定间隔更新的多个 LE密钥31-E的 LE密钥31-D，即以预定间隔更新的多个 LE密钥31-D被用于产生多个 AES解密数据 103。此外，该多个 AES解密数据 103被分别用于加密AV数据的相关部分(相关帧)。

状态呈现部分 74根据是否从元数据提取部分 72提供 (产生)密钥未发现信号 101和加密输入信号 102来识别投影仪4的当前状态，并且呈现所获得的识别结果给投影仪4的用户 (例如再现电影的人

员)。

在本实施例中，以下第一到第三状态被定义成投影仪4的当前状态。

第一状态是加密 AV数据被接收和正常解密的状态 (此后被称作加密输入正常状态)。当密钥未发现信号 101未被提供 (Lo水平)并且加密输入信号 102被提供 (Hi水平)时，投影仪4的当前状态被识别为加密输入正常状态。

第二状态是加密 AV数据被接收但是错误解密的状态 (此后被称作加密输入差错状态)。当密钥未发现信号 101被提供 (Hi水平)并且加密输入信号 102被提供 (Hi水平)时，投影仪4的当前状态被识别为加密输入差错状态。

第三状态是非加密 AV数据被接收的状态 (此后被称作非加密输入状态)。当加密输入信号 102未被提供 (Lo水平)时，投影仪4的当前状态被识别为非加密输入状态。

状态呈现部分 74使用的呈现方法没有特别限制。例如，可以显示图像或产生音频输出。然而，本实施例假定状态呈现部分 74具有以 2种不同颜色照亮的灯，更具体地，是例如以红和绿色照亮的灯，状态呈现部分 74使用以下呈现方法。在本实施例中，灯在加密输入正常状态下以绿色照亮，在加密输入差错状态下以红色照亮，并且在非加密输入状态下熄灭 (关闭)。这允许投影仪4的用户 (例如再现电影的人员)容易地实时监视 3个不同状态。

切换部分 75根据是否从元数据提取部分 72提供加密输入信号 102 (根据水平是 Hi还是 Lo)来切换其输入。

更具体地，当从元数据提取部分 72提供加密输入信号 102时 (当水平为 Hi时)，这意味着加密 AV数据被接收器部分 71接收 (加密输入正常状态或加密输入差错状态成立)。在这种情况下，切换部分 75切换到来自 AV数据解密部分 92的输入。 当加密AV数据被 AV数据解密部分 92解密时获得的恢复 AV数据接着被输入到切换部分 75，并且提供给帧存储部分 77和切换部分 79 (然而，如果加密输入

差错状态成立，则获得噪声数据而不是恢复的 AV数据)。

另一方面，当从元数据提取部分 72未提供加密输入信号 102时(当水平为 Lo时)，这意味着非加密 AV数据被接收器部分 71接收(非加密输入状态成立)。在这种情况下，切换部分 75切换到来自接收器部分 71的输入。 非加密AV数据接着被输入到切换部分 75并且提供给帧存储部分 77和切换部分 79。

如上所述，能够理解，当接收器部分接收非加密 AV数据时，切换部分 75能够禁止解密部分 73执行解密过程 (禁止执行解密过程)。

在加密输入差错状态中，如上所述，从 AV数据解密部分 92输出噪声数据。如果噪声数据被用于再现目的，则在屏幕等等上出现恶劣的图像 (噪声图像)。因此，本实施例在加密输入差错状态将替代图像投影到屏幕等等上。替代图像 (此后被称作固定图像)是预定图案图像或包含消息"等待一会"的图像。

固定图像的图像数据 (此后被称作固定图像数据)被存储在固定图像存储部分 76中。

在本实施例中，作为刚再现的电影、预告片或广告的帧的预定静止图片可以被用作要在加密输入差错状态下投射到屏幕等等上的替代图像。这种帧的帧数据被存储在帧存储部分 77中。换言之，帧存储部分 77存储在从切换部分 75提供的 AV数据中最后提供的帧数据。

然而在加密输入差错状态下，加密数据未被正常恢复，并且变为如上所述的噪声数据。此外，所得到的噪声数据被提供给帧存储部分 77。 如上所述，帧存储部分 77的存在目的是将预定帧数据 (静止图片数据)存储为加密输入差错状态下要投射到屏幕等等上的替代图像而不是噪声数据。如果帧存储部分 77存储噪声数据，则无法实现其目的。

同样地，帧存储部分 77检查是否提供密钥未发现信号 101 (水平为 Hi或 Lo)。当密钥未发现信号 101被提供 (水平为 Hi)时，帧存储部分 77确定从切换部分 75提供噪声数据并且禁止存储这种数据。

结果，在提供密钥未发现信号 101的第一时间点 (此时水平从 Lo改变到 Hi)和不再提供密钥未发现信号 101的第二时间点 (此时水平从Hi改变回到Lo)之间的时间间隔期间，帧存储部分77连续存储紧接在该第一时间点之前提供的正常帧数据(正常静止图片数据)。

根据投影仪4的用户 (例如再现电影的人员)执行的操作 (操作控制部分未被示出)，切换部分 78切换到来自固定图像存储部分 76或帧存储部分 77的输入。

当切换部分 78切换到来自固定图像存储部分 76的输入时，固定图像数据被输入到切换部分 78并且提供给切换部分 79。另一方面，当切换部分 78切换到来自帧存储部分 77的输入时，帧数据被输入到切换部分 78并且提供给切换部分 79。

切换部分79根据是否从元数据提取部分 72提供密钥未发现信号 101(根据水平是 Hi还是 Lo)来切换其输入。

更具体地，当没有从元数据提取部分 72提供密钥未发现信号 101 (水平为 Lo)时，这意味着加密输入正常状态或非加密输入状态成立。在这种情况下，切换部分 79切换到来自切换部分 75的输入。电影的恢复 AV数据或预告片和广告的非加密AV数据接着被输入到切换部分 79，并且提供给再现控制部分 80。

另一方面，当从元数据提取部分 72提供密钥未发现信号 101 (水平为 Hi)时，这意味着加密输入差错状态成立，即从切换部分 75输出噪声数据。在这种情况下，切换部分 79切换到来自切换部分 78的输入。匿定图像数据或帧数据 (对应于电影、预告片或广告图像的帧的数据)接着被输入到切换部分 79，并且提供给再现控制部分 80。

再现控制部分 80控制对应于从切换部分 79提供的内容数据的内容的再现。

在本实施例中，内容数据和内容如下所述。

当切换部分 79已经切换到来自切换部分 75的输入时，即当加密输入正常状态或非加密输入状态成立时，内容数据表示 AV数据，而内容表示对应于该 AV数据的电影、预告片或广告。因此，在上述情

况下，再现控制部分 80将对应于 AV数据的视频，即电影、预告片或广告的视频投射到屏幕等等上，并且使扬声器输出对应于 AV数据的音频，即电影、预告片或广告的音频。更准确地说，在加密输入正常状态成立时，再现控制部分 80将电影的视频投射到屏幕等等，并且使扬声器等等输出电影的音频。在非加密输入状态成立时，再现控制部分 80将电影、预告片或广告的视频投射到屏幕等等上，并且使扬声器等等输出相关音频。

另一方面，当切换部分 79已经切换到来自切换部分 78的输入时，即当加密输入差错状态成立时，内容数据表示固定图像存储部分76中存储的固定图像数据或帧存储部分 77中存储的帧数据。 内容表示对应于固定图像数据的固定图像 (预定图案图像或包含消息"等待一会"的图像)或对应于帧数据的帧 (电影、预告片或广告图像的帧)。因此，在这种情况下，再现控制部分 80行使控制，使得预定图案图像或包含消息"等待一会"的图像被投射到屏幕等等上，或者电影、预告片或广告图像的帧被连续投射到屏幕等等上(投射冻结图像)。

如上所述，当加密输入差错状态成立时，切换部分 79能够将替代图像投射到屏幕等等上，直到差错消失 (直到加密输入正常状态成立），同时防止再现噪声数据。

此外，切换部分 78能够允许投影仪4的用户 (例如再现电影的人员)自由选择作为替代图像投射到屏幕等等上的固定图像或视频的最后帧 (冻结图像)。

现在将参照图9详细描述图8示出的元数据提取部分72。图9示出了元数据提取部分 72的典型配置的详细。

在图9示出的例子中，元数据提取部分72包含元数据提取/分离部分121、 LEKP恢复部分122、 LEKP表123、密钥改变触发器产生部分124、寄存器 125、 126、 128、计数器 127和 AES输入产生部分129。

元数据提取/分离部分121确定元数据34是否被叠加在从接收器部分71提供的 AV数据的预定部分 (参见图3)上。

如果所获得的确定结果指示没有叠加元数据34，则元数据提取/分离部分121认为从接收器部分71接收非加密 AV数据，禁止产生加密输入信号 102 (启动 Lo水平)并且禁止元数据提取部分72执行处理。

另一方面，如果所获得的确定结果指示叠加元数据34，则元数据提取/分离部分121从构成 AV数据的各种帧 (数据)中的相关帧中提取元数据34和其它信息。

接着，元数据提取/分离部分121确认写入元数据34-3中的当前密钥ID值，元数据34-3是包含元数据34-1到 34-3 (参见图4到 6)的元数据34的一部分。

如果写入的当前密钥ID值是特殊值 (例如 0)，则元数据提取/分离部分121认为从接收器部分71接收非加密 AV数据，禁止加密输入信号 102的产生 (启动 Lo水平)，并且禁止元数据提取部分72执行处理。

另一方面，如果写入的当前密钥ID值是不同于特殊值 (例如 0)的值，则元数据提取/分离部分121认为从接收器部分71接收加密 AV数据，产生加密输入信号 102 (启动 Hi水平)，并且提供产生的信号到状态呈现部分 74和切换部分 75 (图8)。 此外，元数据提取/分离部分121分离构成元数据34的各种信息项，并且提供它们到相关模块。

在图9示出的例子中，元数据提取/分离部分121提取或分离LEKM 141、当前LE_Key ID 142、下一LE_Key ID 143、密钥改变定时145、当前帧计数148、帧/线复位150和 HD-SDI链路数152。

帧/线复位150包含帧复位146和线复位151。如前所述， LEKM 141是针对元数据34-1和 34-2的写入用户数据值。当前LE_Key ID 142是针对元数据34-3的写入当前密钥ID值。下一LE_Key ID 143是针对元数据34-3的写入下一密钥ID值。密钥改变定时145是针对元数据34-3的写入密钥改变定时值。HD-SDI链路数152是针对元数据34-3的写入HD-SDI链路数值。当前帧计数148是针对元数据34-3的写入当前帧计数值。

LEKM 141被提供给LEKP恢复部分122。当前LE_Key ID 142和下一LE_Key ID 143被提供给 LEKP表123。密钥改变定时145被提供给密钥改变触发器产生部分124。当前帧计数148被提供给寄存器126。帧复位146被提供给密钥改变触发器产生部分124。线复位151被提供给计数器 127。包含帧复位146和线复位151的帧/线复位150作为图8示出的帧复位33-D被提供给解密部分 73。 HD-SDI链路数152被提供给寄存器 128。

LEKP恢复部分122从 LEKM 141恢复 LEKP，并且在 LEKP表123中存储 LEKP及其密钥ID等等之间的关联。换言之， LEKM 141是针对图4示出的元数据34-1和图5示出的元数据34-2的写入用户数据值，如前所述。用户数据包含 ELEKP (在图4和 5中表示为"Elekp数据")。如前所述， ELEKP是当对 LEKP执行 RSA加密过程时获得的数据。因此，LEKP恢复部分122通过使用公开密钥的配对密钥 (私有密钥)产生 ELEKP，对 LEKM 141中包含的 ELEKP执行解密过程，并且在 LEKP表123中存储所得到的 LEKP (解密的 LEKP)及其密钥ID等等之间的关联。

如上所述， LEKP表123存储一或多个 LEKP和 LEKP识别密钥 ID等等之间的关联。LEKP表123中存储的每个 LEKP包含 LE密钥31-D (图2示出的恢复的 LE密钥31-E)和某些补充信息段。本实施例假定补充信息包含作为图2示出的 AES输入32-E的单元的Le_attribute_data 144。 当寄存器 125发出请求时（按照密钥改变指令提交之后的预定定时，后面会描述)， LEKP表123使寄存器 125存储具有与当前LE_Key ID 142相同的密钥 ID的LEKP中包含的 LE密钥31-D (此后被称作当前 LE密钥31-D)，以及 Le_attribute_data 144 (此后被称作当前 Le_attribute_data 144)。

具有与下一LE_Key ID 143相同的密钥ID的LEKP中包含的LE密钥31-D此后被称作下一 LE密钥31-D。该Le_attribute_data 144此后被称作下一 Le_attribute_data 144。

当具有与当前LE_Key ID 142相同的密钥ID的 LEKP不存在时，

即当当前 LE密钥31-D不存在时， LEKP表123认为当前 LE密钥31-D没有正常地被 LEKP恢复部分122产生 (没有恢复相关 LE密钥31-E)，即解密密钥没有被寄存，产生密钥未发现信号101 (启动Hi水平)，并且提供产生的信号到状态呈现部分74、帧存储部分77和切换部分79 (图8)。

另一方面，当具有与当前LE_Key ID 142相同的密钥ID的 LEKP存在时，即当当前 LE密钥31-D存在时， LEKP表123认为当前 LE密钥31-D被 LEKP恢复部分122正常产生 (相关 LE密钥31-E被恢复)，即解密密钥被寄存，并且禁止产生密钥未发现信号101 (启动 Lo水平)。

每当提供帧复位146时，密钥改变触发器产生部分124提供密钥改变触发器147到寄存器125。更具体地，密钥改变指令和密钥改变禁止指令作为密钥改变触发器147存在，并且这些指令中的任意一个被提供给寄存器125。密钥改变触发器产生部分124监视密钥改变定时145的值。当监视的值为 2'b00 (＝0)时，即当相关帧充当密钥改变定时时，密钥改变触发器产生部分124提供密钥改变指令到寄存器125，以作为密钥改变触发器147。当监视的值为不同于 2'b00 (＝0)的值时，密钥改变触发器产生部分124提供密钥改变禁止指令到寄存器125，以作为密钥改变触发器147。

寄存器125存储当前LE密钥31-D和当前 Le_attribute_data 144。

对于作为密钥改变触发器125提供的密钥改变禁止指令，寄存器125提供当前LE密钥31-D给解密部分73，并且提供当前Le_attribute_data 144给 AES输入产生部分129。解密部分73接着使用当前LE密钥31-D解密相关帧 (AES加密的帧数据)。

另一方面，当作为密钥改变触发器147提供密钥改变指令时，寄存器125请求 LEKP表123更新存储的内容。

LEKP表123接着使寄存器125存储当该请求被寄存器125发出时的当前LE密钥31-D (从寄存器125中作为当前LE密钥31-D存储的 LE密钥31-D观察到的下一 LE密钥31-D）和当前 Le_attribute_data 144

(从寄存器125中作为当前 Le_attribute_data 144存储的Le_attribute_data 144观察到的下一 Le_attribute_data 144)。

换言之，当从密钥改变之前的当前LE密钥31-D和当前Le_attribute_data 144观察时，下一 LE密钥31-D和下一Le_attribute_data 144作为密钥改变之后的新当前LE密钥31-D和新当前 Le_attribute_data 144被存储在寄存器125中。

接着，将新当前LE密钥31-D (曾经是下一 LE密钥31-D)提供给解密部分73，并且将新当前 Le_attribute_data 144 (曾经是下一Le_attribute_data 144)提供给 AES输入产生部分129。

因此，在解密部分73中，用于解密的 LE密钥31-D被从当前LE密钥31-D更新到下一 LE密钥31-D (新当前LE密钥31-D)，以便解密相关帧 (AES加密的帧数据)。

寄存器 126可以保存当前帧计数148并且可以将其提供到 AES输入产生部分129。

每当提供线复位151时，计数器 127将其计数递增一，并且提供所得到的计数给 AES输入产生部分129。

寄存器 128保存HD-SDI链路数152并且将其提供到 AES输入产生部分129。

如上所述， AES输入产生部分129输入来自寄存器125的Le_attribute_data 144，来自寄存器126的当前帧计数148，来自元数据提取/分离部分121的 HD SDI 149的线数，计数器127达到的计数和来自寄存器128的 HD-SDI链路数152。AES输入产生部分129接着产生 AES输入32-D (通过恢复图2示出的 AES输入32-E)，其至少包含Le_attribute_data 144、当前帧计数148、 HD SDI 149的线数、计数器127达到的计数和 HD-SDI链路数152，并且提供产生的 AES输入32-D给解密部分73。

已经参照图1到 9描述了图1示出的发送/接收系统的典型配置。现在描述发送/接收系统执行的操作。

电影院服务器1加密电影的 AV数据并且将其发送到路由器3。

本实施例使用高速执行加密与解密处理的 AES加密方法，以作为用于加密电影的 AV数据的方法。如图2所示配置电影院服务器1。

为产生作为用于 AES加密的代码的 AES加密数据35，图2示出的元数据产生部分13以预定更新间隔顺序产生不同 LE密钥31-E。AES加密数据产生部分21使用顺序产生的 LE密钥31-E和相关 AES输入32-E顺序地产生多个 AES加密数据35。换言之，AES加密数据产生部分21顺序更新 AES加密数据35。

通过使用顺序更新的 AES加密数据35中的每个， AV数据加密部分22以单个帧的方式对从 AV数据存储部分11提供的 AV数据执行AES加密过程。从 AV数据加密部分22向叠加部分14提供所得到的加密 AV数据。

将顺序更新的 LE密钥31-E与某些补充数据(Le_attribute_data 144等等)组合以产生 LEKP。元数据产生部分13通过作为公开密钥密码系统的 RSA加密方法对 LEKP执行加密过程。作为加密过程的结果，获得 ELEKP。由元数据产生部分13针对每个帧产生包含 ELEKP的元数据34，更具体地是本实施例中的元数据34-1到 34-3 (图4到 6)，并且将其提供给叠加部分14。

叠加部分14将元数据34叠加在构成从 AV数据加密部分22提供的加密AV数据的所有帧 (数据)上。在其上以单个帧的方式叠加有元数据34的所得到的加密 AV数据被从叠加部分14提供到发送器部分15，并且接着发送到路由器3。

如上所述，图1示出的电影院服务器1输出电影的加密AV数据并且将其发送到路由器3。

其间，子AV服务器2输出预告片和广告的非加密AV数据并且将其发送到路由器3。

路由器3选择从电影院服务器1提供的加密AV数据或从子AV服务器2提供的非加密AV数据。选择的 AV数据被提供给投影仪4。

选择的 AV数据被提供到的投影仪4能够例如根据图10中的流程图执行操作 (处理)。图10的流程图图解了由投影仪4执行的典型过

程。

图10图解了具体涉及相关帧的处理，相关帧是构成 AV数据的多个帧 (数据)中的一个。换言之，针对构成 AV数据的帧 (数据)中的每个独立执行图10示出的处理。更具体地，例如当针对第一帧执行步骤 S4时，可以同时针对第二帧执行步骤 S2。

执行步骤S1以确定图8示出的投影仪4的接收器部分71是否接收 AV数据 (更准确地说，是相关帧；然而在后续图10的说明中将使用术语"AV数据")。

如果在步骤 S1确定结果指示没有接收 AV数据，则处理返回到步骤 S1，其中执行步骤 S1以确定是否接收 AV数据。换言之，重复执行在步骤 S1的确定方法，直到从路由器3发送 AV数据，使得投影仪4保持在处理后备状态。

当 AV数据被从路由器3发送并且被接收器部分71接收时，在步骤 S1获得的确定结果指示 AV数据被接收。当 AV数据被提供给元数据提取部分72等等时，处理前进到步骤 S2。

执行步骤 S2以确定接收器部分71接收并且提供给元数据提取部分72的 AV数据是否被加密。

在本实施例中，如前所述，当元数据34被包含在 AV数据中并且作为当前密钥ID (参见图6)写入的值不同于特殊值 0时，在步骤 S2获得的确定结果指示提供的 AV数据被加密。在其它情况下，在步骤 S2获得的确定结果指示提供的 AV数据未加密。

如果在步骤 S2获得的确定结果指示提供的 AV数据未加密 (没有加密)，则处理前进到步骤 S7。后面会描述在步骤 S7和其它步骤执行的处理。

另一方面，如果在步骤 S2获得的确定结果指示提供的 AV数据被加密，则处理前进到步骤 S3。在这种情况下，加密输入信号 102被产生 (启动 Hi水平)和提供给状态呈现部分74、切换部分 75等等。

执行步骤 S3以确定 LE密钥31-D是否被元数据提取部分72正常准备。

如前所述，在本实施例中，如果对应于当前LE_Key ID 142的 LE密钥31-D被存储在如图9所示的 LEKP表123中，则在步骤 S3获得的确定结果指示 LE密钥31-D被正常准备。如果没有，则在步骤 S3获得的确定结果指示 LE密钥31-D没有被正常准备。

如果在步骤 S3获得的确定结果指示 LE密钥31-D没有被正常准备，则处理前进到步骤 S9。后面会描述在步骤 S9和其它步骤执行的处理。

另一方面，如果在步骤 S3获得的确定结果指示 LE密钥31-D被正常准备，则处理前进到步骤 S4。在这种情况下，禁止产生密钥未发现信号101 (启动 Lo水平)。

在步骤 S4，解密部分73对从接收器部分71提供的加密AV数据执行解密过程。

在上述情况下，如前所述，由于加密输入信号102被连续提供给切换部分75等等 (保持 Hi水平)，则切换部分75已经切换到来自解密部分73的输入。此外，由于密钥未发现信号101的产生被连续禁止 (保持 Lo水平)，切换部分79已经切换到来自切换部分75的输入。因此，作为步骤 S4的结果而获得的恢复的 AV数据 (电影的 AV数据)被从解密部分73输出并且经由切换部分75、 79提供给再现控制部分 80。

在步骤 S5，再现控制部分80再现对应于恢复的 AV数据的电影。

此外，加密输入信号102被连续提供给状态呈现部分74 (保持 Hi水平)，并且连续禁止密钥未发现信号101的提供 (保持 Lo水平)。因此在步骤 S6，状态呈现部分74指示"加密输入正常状态"(本实施例使得灯以绿色照亮)。

然而实际上步骤 S6不在步骤 S5完成之后执行。步骤 S5和 S6独立并且实际上同时地执行。

返回到步骤 S2，如果在步骤 S2获得的确定结果指示提供的 AV数据未加密 (没有加密)，则处理前进到步骤 S7，如前所述。

在上述情况下，禁止产生加密输入信号102和密钥未发现信号101 (启动 Lo水平)。因此，切换部分75切换到来自接收器部分71的输入，

切换部分79切换到来自切换部分75的输入。因此，接收器部分71在步骤 S1接收的非加密AV数据经由切换部分75、 79被提供给再现控制部分80。

因而在步骤 S7，再现控制部分80再现对应于非加密AV数据的预告片和广告。

连续禁止对状态呈现部分74的加密输入信号102的提供 (保持Lo水平)。因此在步骤 S8，状态呈现部分74指示"非加密输入状态"(本实施例熄灭灯)。

然而实际上步骤S8不在步骤 S7完成之后没有执行。步骤 S7和S8独立并且实际上同时地执行。返回到步骤 S3，如果在步骤 S3获得的确定结果指示 LE密钥31-D没有正常准备，则处理前进到步骤 S9，如前所述。

在上述情况下，如前所述，密钥未发现信号101的产生开始进行，并且接着继续进行 (保持 Hi水平)。切换部分79接着切换到来自切换部分 78的输入。 因此，固定图像存储部分76中存储的固定图像数据或帧存储部分77中存储的帧数据经由切换部分78、 79被提供给再现控制部分80。

因而在步骤 S9，再现控制部分80再现预定帧 (静止图片)或固定图像。

密钥未发现信号101和加密输入信号102均被连续提供给状态呈现部分74 (两个信号的水平均连续为 Hi)。因此在步骤 S10，状态呈现部分74指示"加密输入差错状态"(本实施例使得灯发出红光)。

然而实际上步骤S10不在步骤 S9完成之后没有执行。步骤 S9和S10独立并且实际上同时地执行。已经描述了图1示出的发送/接收系统执行的操作。

本发明不仅适用于图1示出的发送/接收系统，而且适用于各种其它系统。在图1示出的例子 (图2示出的例子)中， LE密钥31-E被包含在元数据34中，元数据4被叠加在加密 AV数据上并且从作为发送端的电影院服务器1发送到作为接收端的投影仪4。 换言之， LE密钥

31-E与加密AV数据一起发送。然而 LE密钥31-E不需要与加密AV数据一起发送。本发明也可以适用于这样的发送/接收系统，其中通过不同传输路径从发送端向接收端发送 LE密钥31-E和加密 AV数据。图11示出了这种发送/接收系统的典型配置。 图11的模块图图解了根据本发明实施例的发送/接收系统的另一典型配置，其不同图1示出的配置。

对于图11示出的发送/接收系统的与图1中相同的单元，为其分配相同的附图标记并且根据情况省略其描述。

在图11示出的例子中，发送/接收系统包含电影院服务器201、子AV服务器2、路由器3和投影仪202。

图1和 11示出的例子之间的比较表明，图1示出的例子 (图2示出的例子）内的电影院服务器1处理包含 LE密钥31-E的元数据34，在加密 AV数据上叠加元数据34，并且经由路由器3向投影仪4发送所得到的组合。

另一方面，图11示出的例子内的电影院服务器201经由预定网络203向投影仪202发送 LE密钥31-E及其密钥ID的组合 (这个组合此后被称作 LE密钥+密钥ID 211)。

如上所述，图11示出的例子不同于图1示出的例子的地方在于前者通过不同路径发送 LE密钥31-E和加密 AV数据。在其它方面，图11示出的例子与图1示出的例子基本相同。因此，图11示出的发送 LE密钥31-E的电影院服务器201具有的配置略微不同于图1示出的电影院服务器1的配置例子 (图2)。 出于同样原因，图11示出的接收 LE密钥31-E的投影仪202具有的配置略微不同于图1示出的投影仪4的配置例子 (图8)。

例如，可以分别如图12和 13所示配置电影院服务器201和投影仪202。图12图解了电影院服务器201的典型配置。图13图解了投影仪202的典型配置。对于图12示出的电影院服务器201的与图2示出的电影院服务器1相同的单元，为其分配相同的附图标记并且根据情况省略其描述。类似地，对于图13示出的投影仪202的与图8示出的投影仪4相

同的单元，为其分配相同的附图标记并且根据情况省略其描述。

在图12示出的例子中，电影院服务器201包含 AV数据存储部分11、加密部分12和叠加部分14，这些部分与图2示出的电影院服务器1的那些部分相同。 然而，图12示出的电影院服务器201也包含元数据产生部分221、 AV发送器部分222和密钥发送器部分223，这不同于图2示出的电影院服务器1。

下面将只描述不同于图2示出的电影院服务器1的那些单元的单元，即只描述元数据产生部分221、 AV发送器部分222和密钥发送器部分223。

元数据产生部分221产生用于加密部分12的加密过程的各种信息(即用于投影仪202的解密过程的各种信息)，更具体地是如前所述的LE密钥31-E、 AES输入32-E、帧复位 33 - 3等等，并且向加密部分12提供产生的信息。

迄今为止执行的处理与图2示出的元数据产生部分13执行的处理基本相同。然而后续处理略微不同于由图2示出的元数据产生部分13执行的处理。

更具体地，元数据产生部分221在内置 LE密钥表221-1中存储作为产生的 LE密钥31-E及其密钥ID的组合的 LE密钥+密钥ID 211。因此， LE密钥表221-1存储一或多组 LE密钥+密钥ID 211。

LE密钥+密钥ID 211是涉及发送/接收系统的安全性的密钥信息。因此，需要防止 LE密钥+密钥ID 211被窃用，虽然它存在于电影院服务器201之内。在这种情况下， LE密钥+密钥ID 211应当在被存储在LE密钥表221-1中之前加密。对加密 LE密钥+密钥ID 211的方法没有特别限制。

对 LE密钥表221-1中要准备和存储的 LE密钥+密钥ID 211的组的数量也没有特别限制。这取决于更新 LE密钥31-E的间隔和各种其它发送/接收系统操作策略。在 LE密钥表221-1中可以准备和存储任何数量的 LE密钥+密钥ID 211的组，只要其符合操作策略。

LE密钥表221-1中存储的一或多个组的 LE密钥+密钥ID 211被

单独发送到密钥发送器部分223。

此外，将除了 LE密钥+密钥ID 211之外的各种信息 (例如图6示出的元数据34-3中包含的信息)作为元数据 224提供给叠加部分14。在这种情况下，元数据 224可以经过RSA加密，或仍未加密，因为它不包含需要保护的 LE密钥31-E。

然而上述处理略微不同于由图2示出的元数据产生部分13执行的处理。

在叠加部分14中，元数据被叠加在加密AV数据上，无论叠加发生在图2示出的例子中还是图12示出的例子中。 然而，图12示出的例子中叠加的元数据不同于图2示出的例子中叠加的元数据。 如前所述，在图2示出的例子中，元数据34被叠加在加密AV数据上。另一方面，在图12示出的例子中，元数据 224被叠加在加密AV数据上。

AV发送器部分222经由路由器3向投影仪202发送从叠加部分14提供的加密AV数据，即在其上叠加有元数据 224的加密AV数据，更具体地是不包含 LE密钥31-E的加密AV数据。

其间，密钥发送器部分223经由网络 203向投影仪202发送 LE密钥表221-1中存储的 LE密钥+密钥ID 211。

密钥发送器部分223的 LE密钥+密钥ID传输定时是在用相关LE密钥31-E加密的一部分加密AV数据 (某个数量的帧数据)的传输前面的定时。这是可接受的，只要投影仪202没有延迟地执行解密过程。

为防止由于网络错误或投影仪欺骗而将 LE密钥+密钥ID 211 (相关 LE密钥31-E)公开给第三方，例如通过在密钥发送器部分223用投影仪202的公开密钥建立TLS (传送层安全性)会话(安全通信路径)之后传送LE密钥+密钥ID 211，能够建立经由网络203的投影仪202和电影院服务器201 (密钥发送器部分223)之间的通信。

在图13示出的例子中，与电影院服务器201相关的投影仪202包含AV接收器部分231、密钥接收器部分232和元数据提取部分233，这不同于图8示出的投影仪4。 投影仪202也包含解密部分73、状态呈现部

分74、切换部分75、 78、 79、固定图像存储部分76、帧存储部分77和再现控制部分80，这些与图8示出的投影仪4的单元相同。

下面将只描述不同于图8示出的投影仪4的那些单元的单元，即AV接收器部分231、密钥接收器部分232和元数据提取部分233。

AV接收器部分231从路由器3 (图11)接收 AV数据。 换言之，AV接收器部分231接收来自电影院服务器201 (图11和 12)或的加密AV数据 (在其上叠加没有 LE密钥31-E的元数据 224的加密 AV数据)或来自子AV服务器2的未加密 AV数据。 其间，密钥接收器部分232接收经由网络 203 (图11)从电影院服务器201发送的 LE密钥+密钥ID 211，并且将其提供给元数据提取部分233。

例如能够如图14所示配置元数据提取部分233。图14的模块图图解了元数据提取部分233的典型配置的细节。

对于图12示出的元数据提取部分233的与图9示出的元数据提取部分72相同的单元，为其分配相同的附图标记并且根据情况省略其描述。在图14示出的例子中，元数据提取部分233包含元数据提取/分离部分241、 LEKP表123、密钥改变触发器产生部分124、寄存器 125、126、 128、计数器 127和 AES输入产生部分129。

图9和 14之间的比较表明，图9示出的元数据提取部分72包含LEKP恢复部分122，因为作为恢复目标的 LE密钥31-E (要产生的LE密钥31-D)被包含在从接收器部分71提供的加密AV数据上叠加的元数据 (参见图8)中。

另一方面，密钥接收器部分232提供作为恢复目标的 LE密钥31-E (要产生的 LE密钥31-D)给图14示出的元数据提取部分233，以作为 LE密钥+密钥ID 211。因此，图14示出的元数据提取部分233不具有 LEKP恢复部分122，使得从密钥接收器部分232提供的 LE密钥+密钥ID 211被直接存储在 LEKP表123中。

如前所述， LE密钥+密钥ID 211是涉及发送/接收系统的安全性并且在加密 AV数据的发送之前发送的密钥信息。因此，需要防止 LE密钥+密钥ID 211被窃用，虽然它存在于投影仪202之内。在这种情况

下， LE密钥+密钥ID 211应当在被存储在 LEKP表123中之前加密，虽然对加密 LE密钥+密钥ID 211的方法没有特别限制。

元数据提取/分离部分 241确定元数据是否被叠加在从 AV接收器部分231提供的 AV数据的预定部分上 (参见图3；然而用附图标记224替换图3中的附图标记 4)。

如果所获得的确定结果指示没有叠加元数据224，则元数据提取/分离部分241认为从AV接收器部分231接收非加密 AV数据，禁止产生加密输入信号 102 (启动 Lo水平)并且禁止元数据提取部分233执行处理。

另一方面，如果所获得的确定结果指示叠加元数据224，则元数据提取/分离部分241从构成 AV数据的多个帧 (数据)中的相关帧中提取元数据224和其它信息。

接着，元数据提取/分离部分 241确认元数据 224中包含的写入当前密钥ID值 (元数据34-3中的写入当前密钥ID值或对应于它的值)。

如果写入的当前密钥ID值是特殊值 (例如 0)，则元数据提取/分离部分241认为从接收器部分231接收非加密 AV数据，禁止加密输入信号 102的产生 (启动 Lo水平)，并且禁止元数据提取部分233执行处理。

另一方面，如果写入的当前密钥ID值是不同于特殊值 (例如 0)的值，则元数据提取/分离部分241认为从接收器部分231接收加密 AV数据，产生加密输入信号 102 (启动 Hi水平)，并且提供产生的信号到状态呈现部分 74和切换部分 75 (图13)。 此外，元数据提取/分离部分241分离构成元数据224的各种信息项，并且提供它们到相关模块。

在图14示出的例子中，元数据提取/分离部分241提取或分离当前LE_Key ID 142、下一LE_Key ID 143、密钥改变定时145、当前帧计数 148 、帧 / 线复位 150 和 HD-SDI 链路数，以及用于产生Le_attribute_data 144的信息。

当前 LE_Key ID 142、下一 LE_Key ID 143和用于产生

Le_attribute_data 144的信息接着被提供给 LEKP表123。在这种情况下，根据用于产生 Le_attribute_data 144的信息产生Le_attribute_data 144，将其与匹配的 LE密钥+密钥ID 211 (相关 LE密钥31-D)组合，并且存储在 LEKP表123中。密钥改变定时145被提供给密钥改变触发器产生部分124。当前帧计数148被提供给寄存器126。帧复位146被提供给密钥改变触发器产生部分124。线复位151被提供给计数器 127。包含帧复位146和线复位151的帧/线复位150作为图13示出的帧复位33-D被提供给解密部分 73。 HD-SDI链路数152被提供给寄存器 128。

图14示出的元数据提取部分233中的没有描述的单元，即 LEKP表123、密钥改变触发器产生部分124、寄存器125、 126、128、计数器127和 AS输入产生部分 129在这里没有描述，因为它们与图9示出的对应单元具有基本相同的功能和配置。

已经参照图11到14描述了图11示出的发送/接收系统的典型配置。 这里没有描述发送/接收系统执行的操作，因为它们与参照图1描述的操作基本相同，除了与图1示出的对应单元不同的单元所执行的操作 (处理)之外。

如上所述，图1和 11示出的发送/接收系统的作为接收设备的投影仪4 (图8)和投影仪202 (图13)能够产生加密输入信号102。 因此，加密输入信号102的使用允许接收端容易地确定从发送端发送的数字资料 (在上述例子中的电影、预告片或广告的流数据)是否被加密。结果，提供了无论其是否加密均允许接收端容易地处理数字资料的第一优点。

当由于路由器的切换而将非加密流数据输入到投影仪4或投影仪202时，需要执行处理以便与切换定时同步地跳过投影仪4或投影仪202内的解密过程 (解密部分73的处理）。在相反切换时，也需要执行相同处理.当使用现有技术的投影仪时，需要实施外部控制以执行以上处理。然而，本实施例提供了不必进行这种外部控制的第二优点，因为提供切换部分75 (图8和 13)以根据加密输入信号102来改变输入。

由于可以不需要这种外部控制，不必为发送/接收系统提供用于进行这种外部控制的特殊单元。此外，开关或其它简单设备可以被用作切换部分75。结果，提供了易于构造整个发送/接收系统的第三优点。

第二和第三优点不仅能够适用于图1和 11示出的小规模再现信号交换系统 (发送/接收系统)，而且能够适用于包含大量服务器和投影仪的大规模发送/接收系统。特别是，在使用后一系统，即大规模发送/接收系统期间，将加强第三优点。

此外，作为接收设备的投影仪4 (图8)和投影仪202 (图13)能够产生密钥未发现信号101，其指示是否准备了用于加密流数据 (在上述例子中的加密 AV数据)的解密的公共密钥。因此，密钥未发现信号101的使用 (在上述例子中图8和 13示出的切换部分79的使用)使得能够提供第四优点。更具体地，即使由于错误输入要输入到不同投影仪的信号或对加密公共密钥 (上述例子中的 LE密钥31-D)的解密过程被延迟而没有准备公共密钥，也能够防止噪声被输出到投射的图像上(屏幕上图像)。

此外，作为接收设备的投影仪4 (图8)和投影仪202 (图13)配有使用密钥未发现信号101和加密输入信号102的状态呈现部分74。 因此，提供了能够监视投影仪4和投影仪202的状态的第五优点。更具体地，例如可以检查接收的流数据 (上述例子中的 AV数据)是否加密，以及加密流数据 (上述例子中的加密 AV数据)是否正常解密。第五优点(第五优点提供的功能)不仅能够有效用于监视正常操作，而且能够有效用于通过手工改变信号 (流数据)来检查系统。

能够提供上述优点的发送/接收系统，即根据本发明实施例的发送/接收系统不局限于图1和 10示出的例子。 本发明适用于任何至少包含引入如下所述功能的接收设备的发送/接收系统。

换言之，发送/接收系统提供第一到第三优点，只要其能够确定接收器接收的流数据是否被加密，并且产生指示所获得的确定结果的加密信息 (在上述例子中产生加密输入信号102，或产生任何其他指示所获得的确定结果的信息)。

发送/接收系统提供第四优点，只要其在公共密钥将被发送到接收设备时确定在对用公共密钥加密并且由接收器接收的加密流数据执行解密过程之前公共密钥是否被正常准备。作为第四优点，发送/接收系统产生指示所获得的确定结果的公共密钥准备信息 (上述例子中的密钥未发现信号101或任何其他公共密钥准备信息)。

发送/接收系统提供第五优点，只要其根据由上述 2个功能产生的加密信息和公共密钥准备信息识别接收设备的状态，并且呈现所获得的识别结果。

能够输入加密 HD-SDI信号 (上述例子中的加密 AV数据)的投影仪4和投影仪202已经被描述为本发明适用于的接收设备。然而在将来，这种输入能力不仅可以被引入到投影仪中，而且可以被引入到录像带记录器、盘记录器、交换机、监视器和各种其它设备中。当它们额外引入提供第一到第五优点的各种功能时，具有这种输入能力的设备能够充当根据本发明实施例的接收设备。当各种设备被实现成本发明适用于的接收设备时，可发现将能够更加容易地使用发送/接收系统。

在上述例子中，本发明适用于的发送/接收系统发送的流数据通过公共密钥密码系统进行加密，并且接着从发送端发送到接收端。因此，也从发送端发送公共密钥 (上述例子中的 LE密钥31-E等等)。在这种情况下，由于公共密钥是涉及发送/接收系统的安全性的密钥信息，需要在其传输期间防止窃用。在这种情况下，上述例子中的公共密钥在从发送端发送到接收端之前进行 RSA加密。

也可以通过不同于 RSA加密方法的各种加密方法加密公共密钥。然而，公开密钥密码系统的使用适于包含上述例子 (RSA加密方法的使用)。原因在于，在基于 RSA加密方法或其它公开密钥密码系统的使用的系统中，私有密钥 (例如用于解密的密钥、加密公共密钥)被如此管理，使得它不泄漏出解密侧 (例如接收设备) (基本通过这种方式管理私有密钥，因为它应当通过这种方式管理)。因此能够使得实际难以窃用私有密钥。甚至更加难以窃用装入 IC (集成电路)卡或芯

片中的私有密钥。换言之，能够使私有密钥窃用的可能性更加接近于0%。

例如，除了上述 RSA加密方法之外，ECC (椭圆曲线密码系统)、ElGamal 、 Rabin 、 Williams、 EPOC 和 NTRU 加密方法可用作公开密钥密码系统。所有这些公开密钥密码系统能够被用作加密公共密钥 (例如上述例子中的 LE密钥31-E)的方法。

上述一系列处理 (例如图10图解的处理)能够通过硬件和通过软件来执行。当该系列处理要通过软件执行时，构成软件的程序被从程序存储介质安装到用专用硬件建立的计算机、通用个人计算机或当安装各种程序时能够执行各种功能的其它计算机中。

图15的模块图图解了执行上述系列处理的个人计算机的典型配置。例如当要通过程序执行图10示出的处理时，具有图15示出的配置的个人计算机可以构成图1示出的投影仪4或图11示出的投影仪202的全部或一部分。

参照图15， CPU (中央处理单元) 301根据 ROM (只读存储器) 302或存储部分 308中存储的程序执行各种处理。要由 CPU 301执行的程序和数据可以被存储在 RAM (随机访问存储器) 303中。CPU 301、 ROM 302和 RAM 303经由总线 304互连。

CPU 301经由总线 304被连接到输入/输出接口 305。输入/输出接口 305被连接到包含键盘、鼠标、话筒等等的输入部分 306，以及包含显示器、投影设备、扬声器等等的输出部分 307。CPU 301根据从输入部分 306输入的指令执行各种处理。CPU 301输出处理结果到输出部分 307。

连接到输入/输出接口 305的存储部分 308是例如硬盘，并且用于存储各种数据和要由 CPU 301执行的程序。通信部分 309经由例如因特网或局域网的网络与外部设备通信。

此外，可以经由通信部分 309获得程序，程序也可以存储在存储部分 308中。

当例如磁盘、光盘、磁光盘、半导体存储器的可折卸介质被插入

到连接到输入/输出接口 305的驱动器 310中时，驱动器 310驱动插入的介质并且获得介质上记录的程序或数据。获得的程序或数据可以被传送到存储部分 308并且存储。

如图15所示，用于存储要安装在计算机上并且可由计算机执行的程序的程序记录介质是可折卸介质 311、 ROM 302或硬盘。可折卸介质 311是包装介质，包含磁盘 (包含软盘)、光盘 (包含CD-ROM [光盘只读存储器] 和 DVD [数字通用光盘])、磁光盘和半导体存储器。ROM 302临时或永久存储程序。硬盘构成存储部分 308。通过使用例如因特网、局域网或数字卫星广播的有线或无线通信介质，可以经由作为针对路由器和调制解调器的接口的通信部分 309将程序存储在程序记录介质上。

在本文中，用于编写要存储在记录介质上的程序的步骤不仅包含按时间先后顺序执行的处理，而且包含并行或单独执行并且不必按时间先后顺序执行的处理。

在本文中使用的术语"系统"表示多个设备的聚集。

本领域的技术人员应当理解，根据设计需求和其它因素，可以进行各种修改，组合，子组合和变化，只要它们在所附权利要求书或其等同表述的范围内。

图1

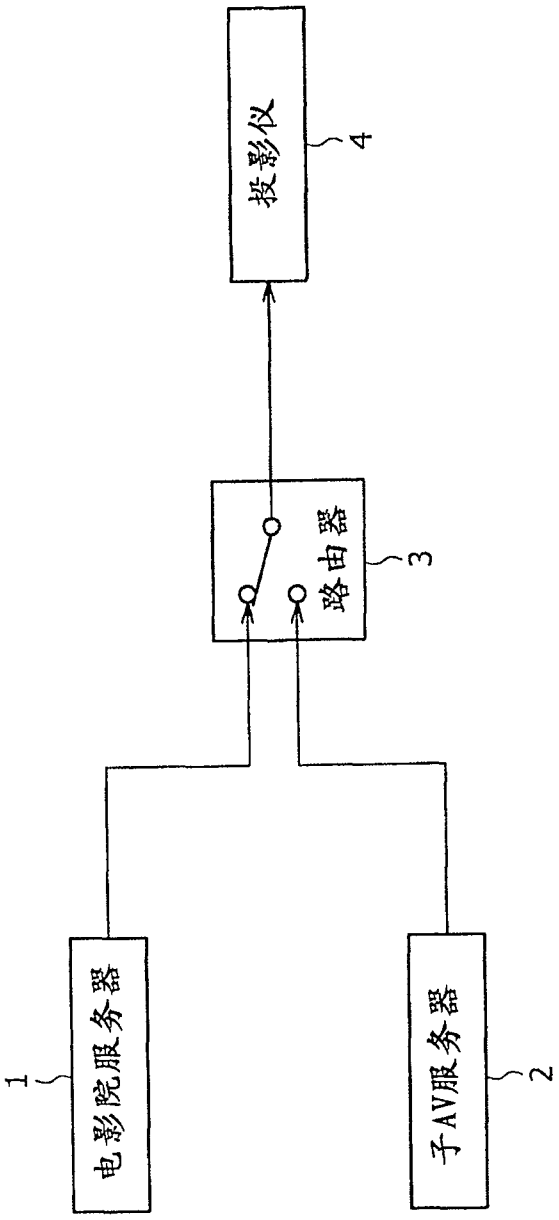


图2

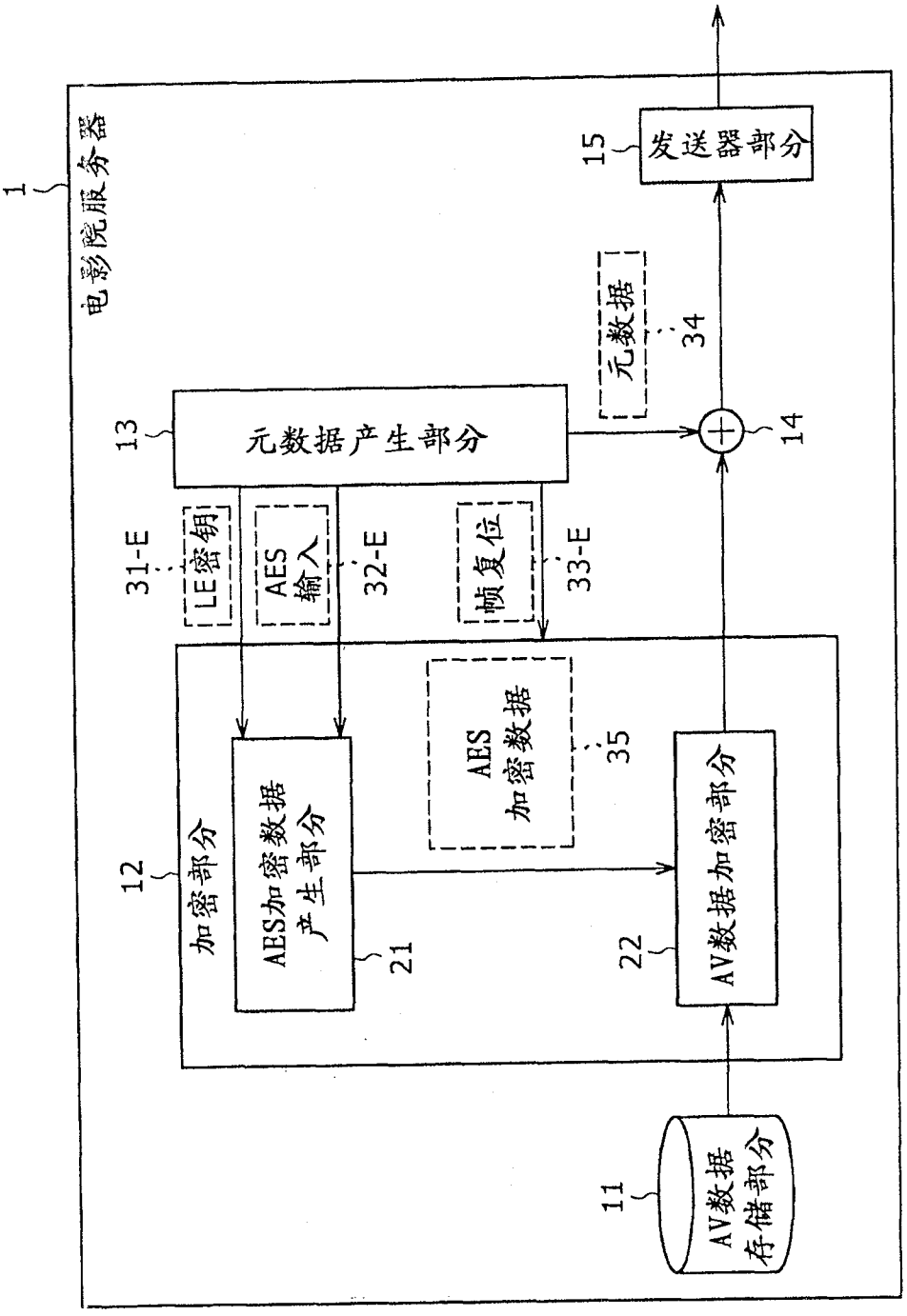
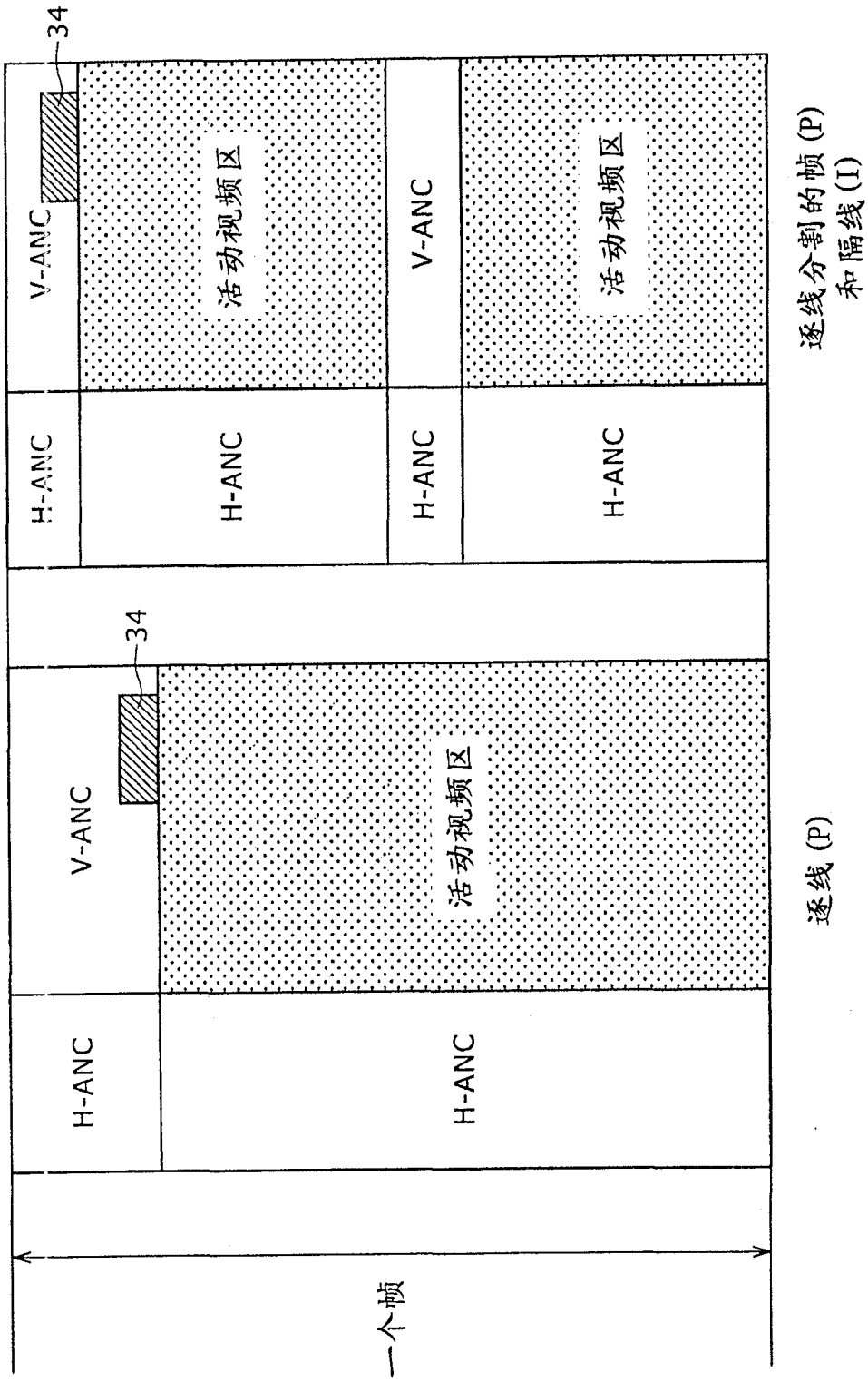

1
电影院服务器
15
发送器部分
元数据
34
13
元数据产生部分
14
31-E
LE密钥
AES
输入
32-E
帧复位
33-E
12
加密部分
AES加密数据
产生部分
21
AES
加密数据
35
22
AV数据加密部分
11
AV数据
存储部分

图 3


34
V-ANC
H-ANC
活动视频区
V-ANC
H-ANC
活动视频区
逐线分割的帧 (P)
和隔线(I)
34
V-ANC
H-ANC
活动视频区
H-ANC
逐线 (P)
一个帧

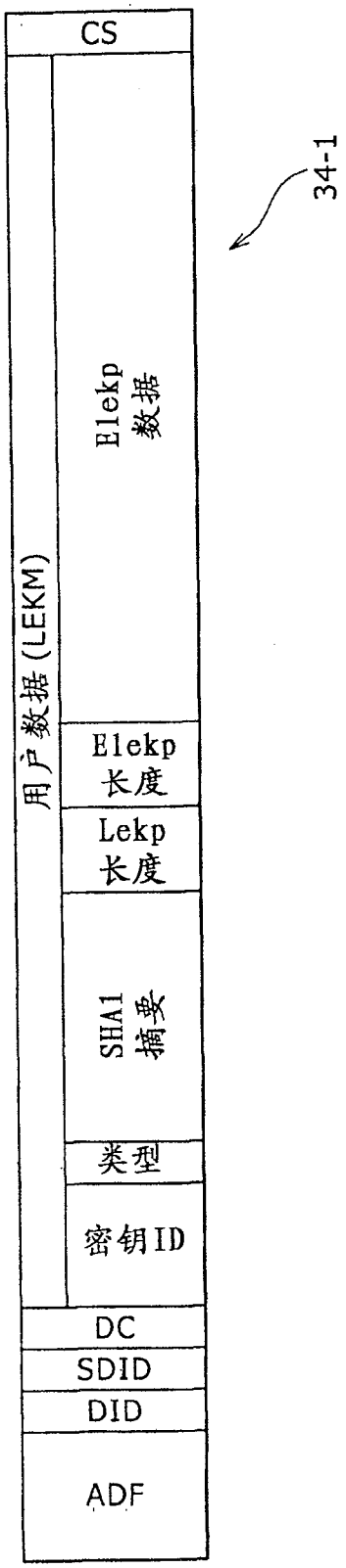

CS
用户数据(LEKM)
Elekp
数据
34-1
Elekp
长度
Lekp
长度
SHA1
摘要
类型
密钥ID
DC
SDID
DID
ADF

图4

图5

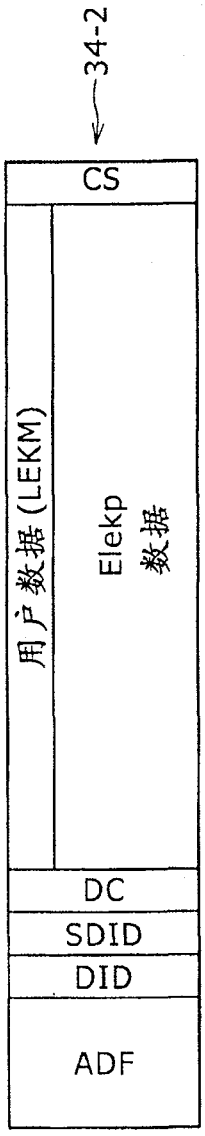


图6

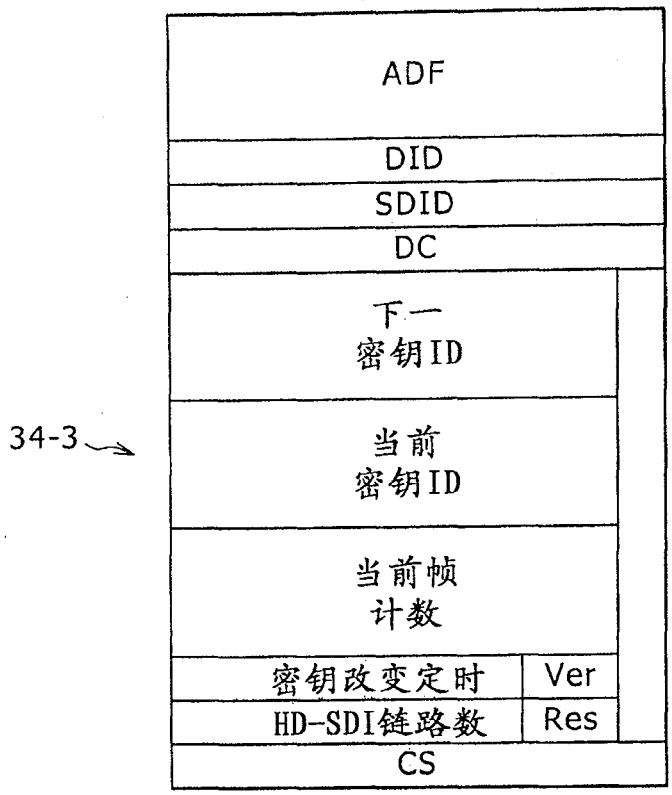

ADF
DID
SDID
DC
下一
密钥ID
34-3
当前
密钥ID
当前帧
计数
密钥改变定时
Ver
HD-SDI链路数
Res
CS

图7

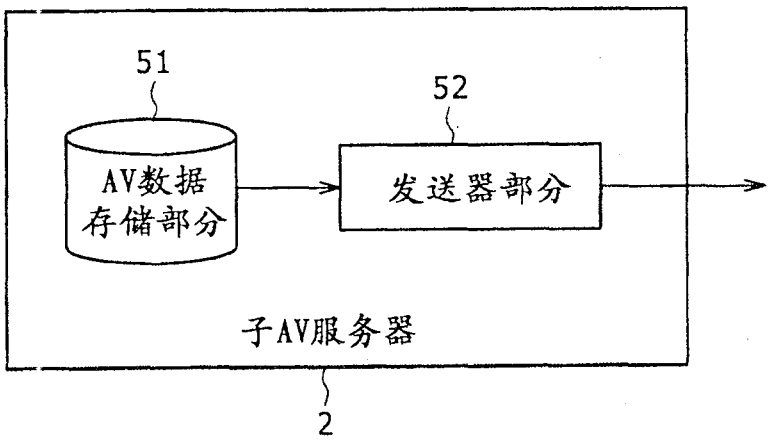

51
52
AV数据
存储部分
发送器部分
子AV服务器
2

图8

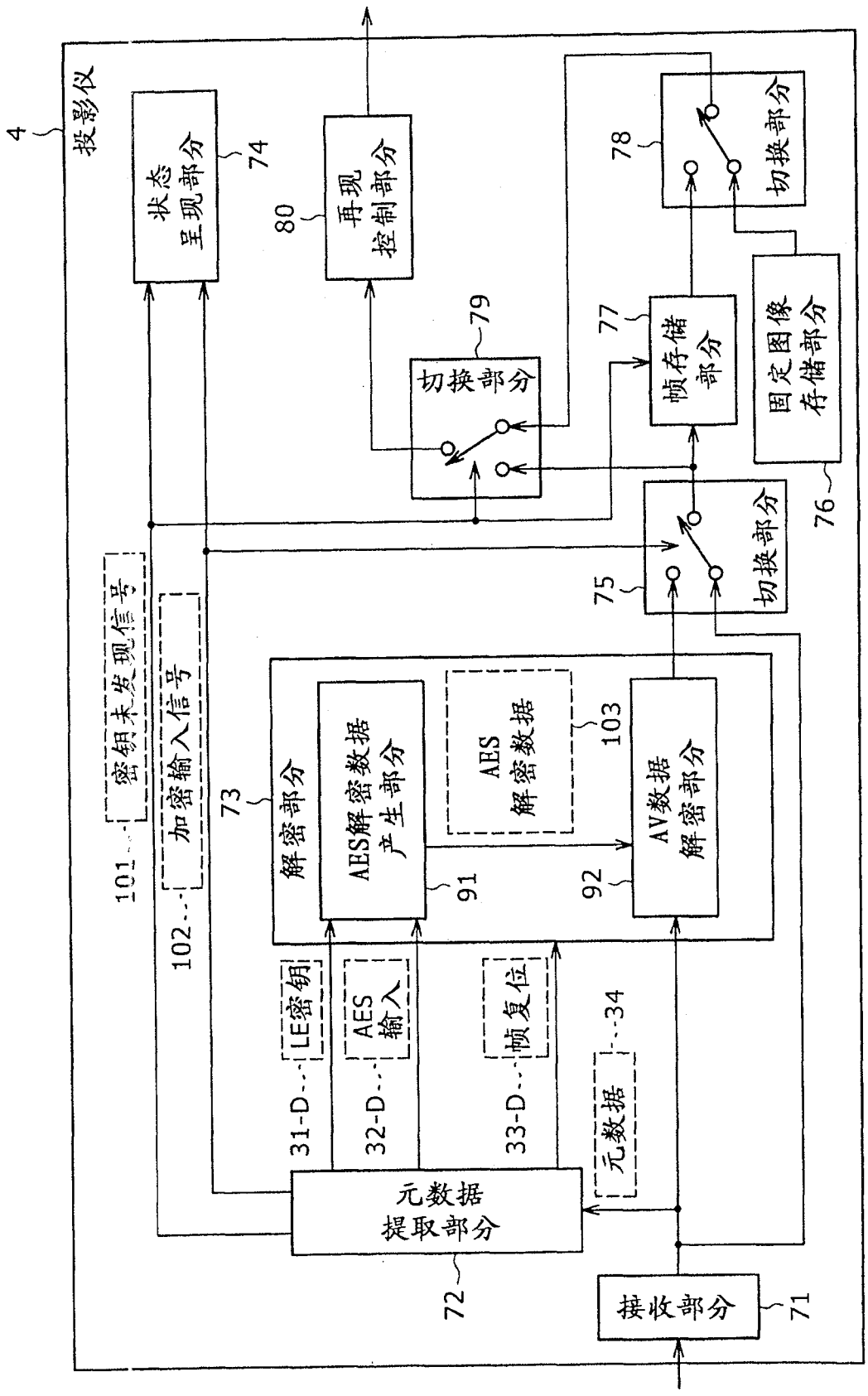

4
投影仪
状态呈现部分
74
80
再现控制部分
78
切换部分
79
77
帧存储部分
固定图像存储部分
76
切换部分
75
101
密钥未发现信号
102
加密输入信号
73
解密部分
AES解密数据产生部分
91
AES解密数据
103
92
AV数据解密部分
31-D
LE密钥
32-D
AES输入
33-D
帧复位
34
元数据
元数据提取部分
72
接收部分
71

图 9

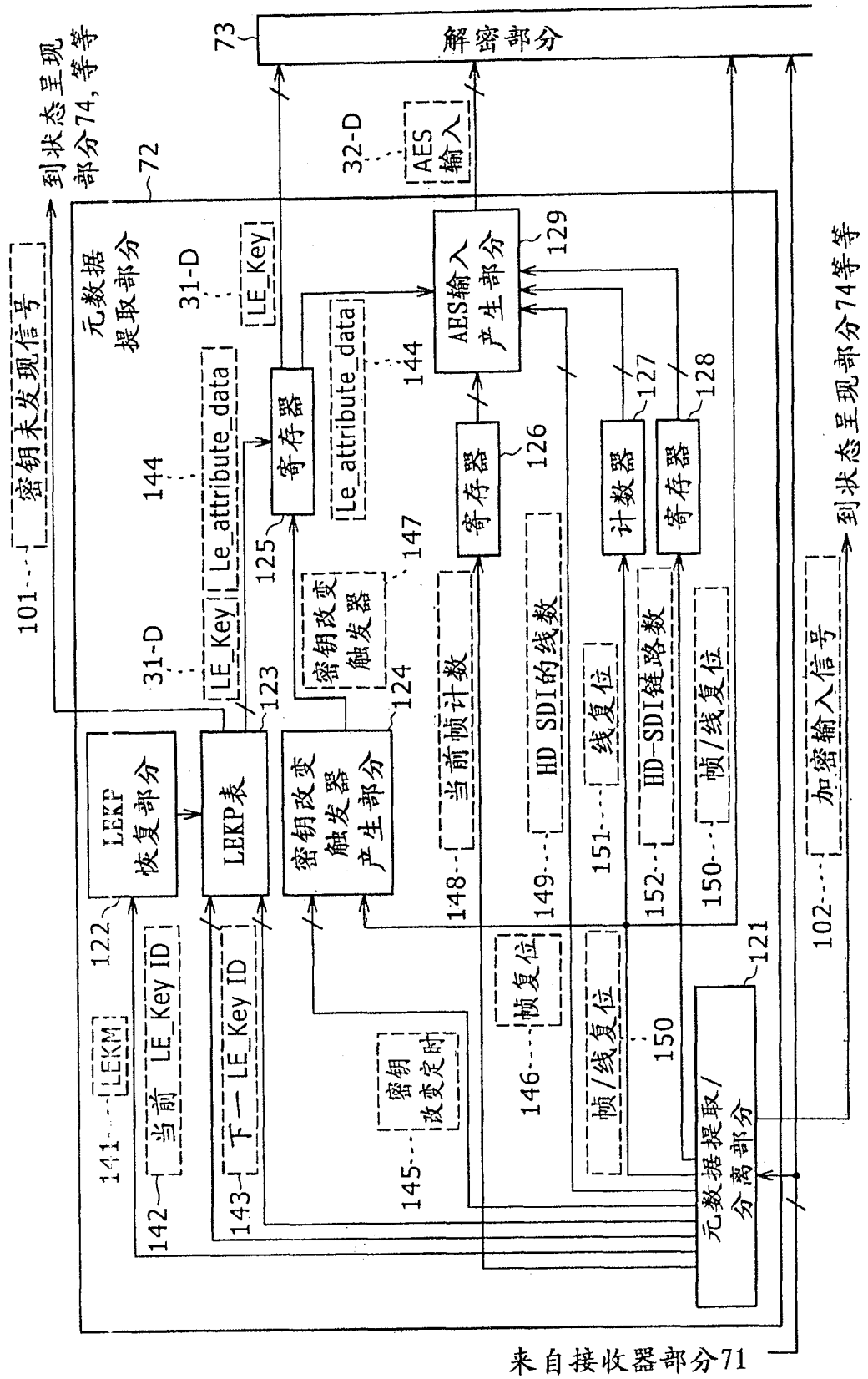

密钥未发现信号
101
到状态呈现部分74,等等
73
解密部分
72
元数据提取部分
31-D
144
Le_attribute_data
LE_Key
32-D
AES输入
LEKP恢复部分
LEKP表
密钥改变触发器产生部分
寄存器
密钥改变触发器
当前帧计数
HD SDI的线数
线复位
HD-SDI链路数
帧/线复位
AES输入产生部分
寄存器
计数器
寄存器
帧复位
帧/线复位
元数据提取/分离部分
加密输入信号
到状态呈现部分74等等
来自接收器部分71
LEKM
当前 LE_Key ID
下一 LE_Key ID
密钥改变定时
122
123
124
125
126
127
128
129
141
142
143
145
146
147
148
149
150
151
152
121
102

图10

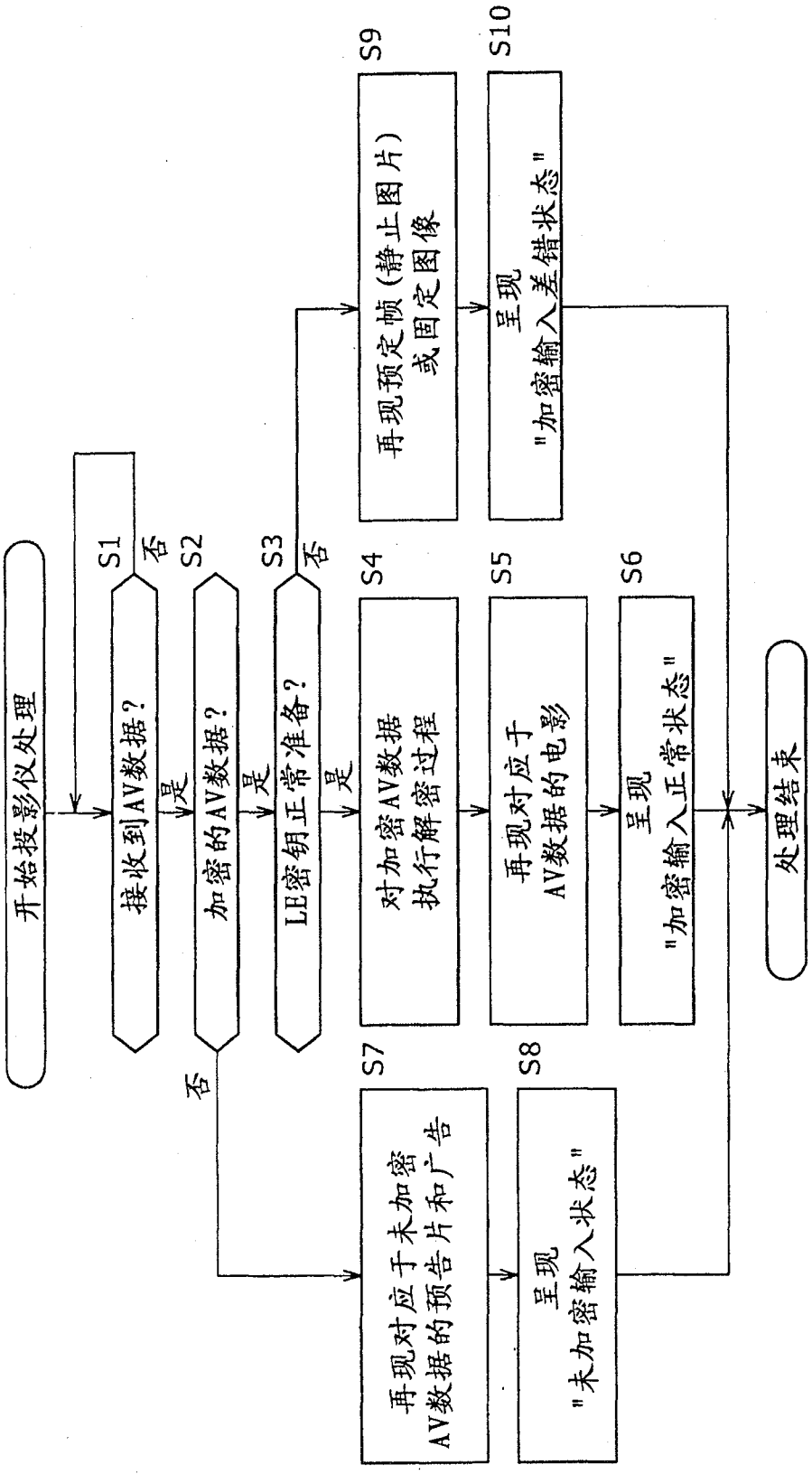

开始投影仪处理
S1
接收到AV数据？
否
是
S2
加密的AV数据？
否
是
S3
LE密钥正常准备？
否
是
S4
对加密AV数据
执行解密过程
S5
再现对应于
AV数据的电影
S6
呈现
"加密输入正常状态"
S7
再现对应于未加密
AV数据的预告片和广告
S8
呈现
"未加密输入状态"
S9
再现预定帧(静止图片)
或固定图像
S10
呈现
"加密输入差错状态"
处理结束

图11

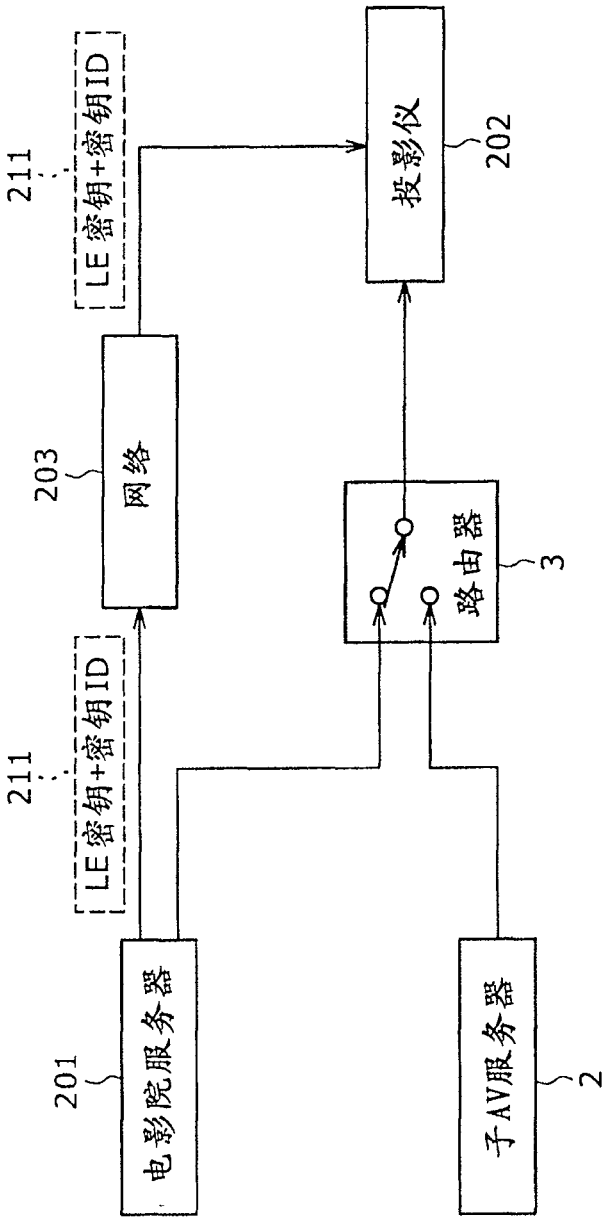

电影院服务器
201
LE密钥+密钥ID
211
网络
203
LE密钥+密钥ID
211
投影仪
202
路由器
3
子AV服务器
2

图12

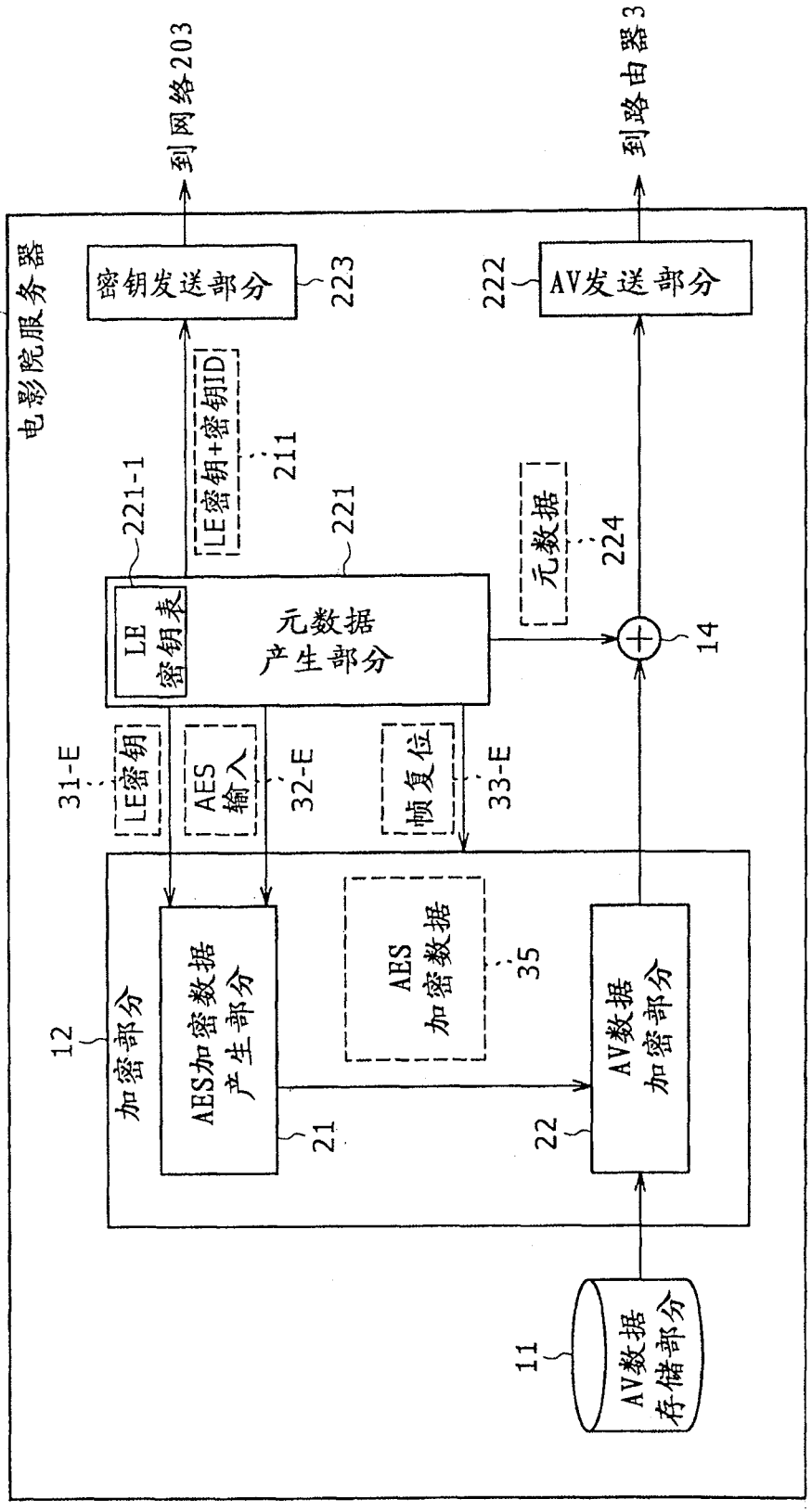

201
电影院服务器
到网络203
到路由器3
密钥发送部分
223
222
AV发送部分
LE密钥+密钥ID
211
221-1
221
LE密钥表
元数据产生部分
元数据
224
14
31-E
LE密钥
AES输入
32-E
帧复位
33-E
12
加密部分
AES加密数据产生部分
21
AES加密数据
35
AV数据加密部分
22
11
AV数据存储部分

图13

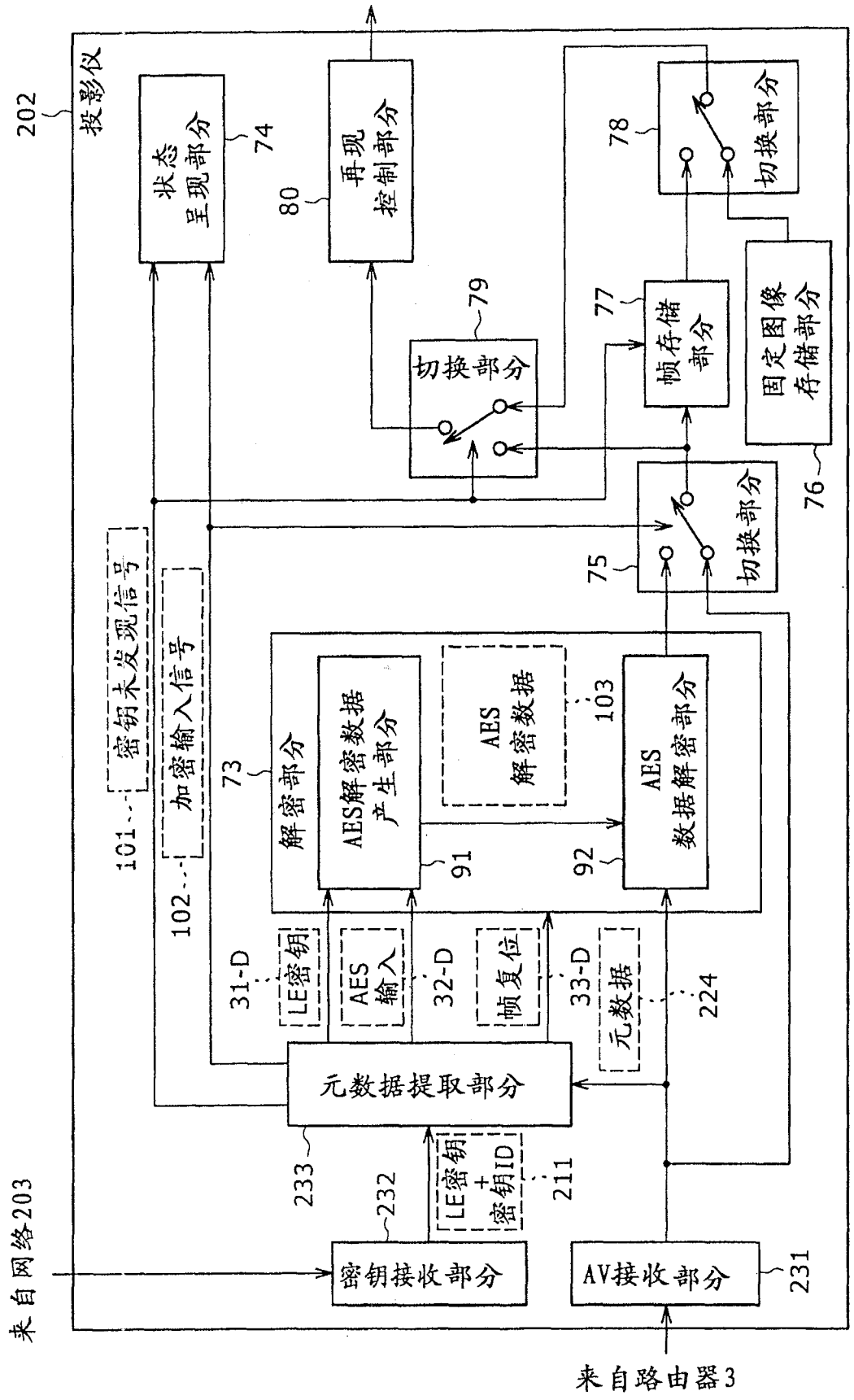

202
投影仪
状态呈现部分
74
80
再现控制部分
78
切换部分
79
切换部分
77
帧存储部分
固定图像存储部分
76
75
切换部分
密钥未发现信号
101
加密输入信号
102
73
解密部分
AES解密数据产生部分
91
AES解密数据
103
92
AES数据解密部分
31-D
LE密钥
AES输入
32-D
帧复位
33-D
元数据
224
元数据提取部分
233
232
LE密钥+密钥ID
211
密钥接收部分
AV接收部分
231
来自网络203
来自路由器3

图14

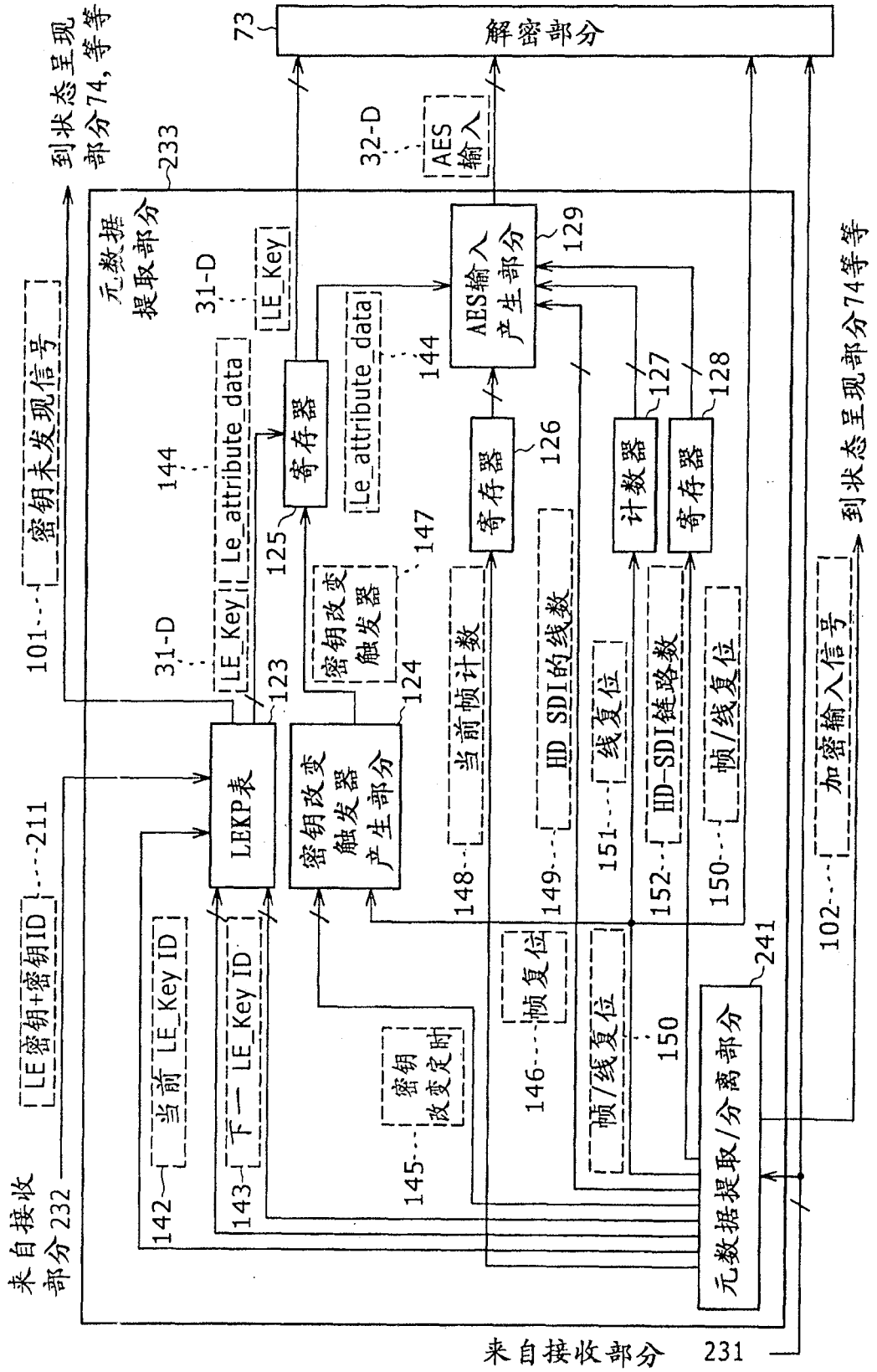
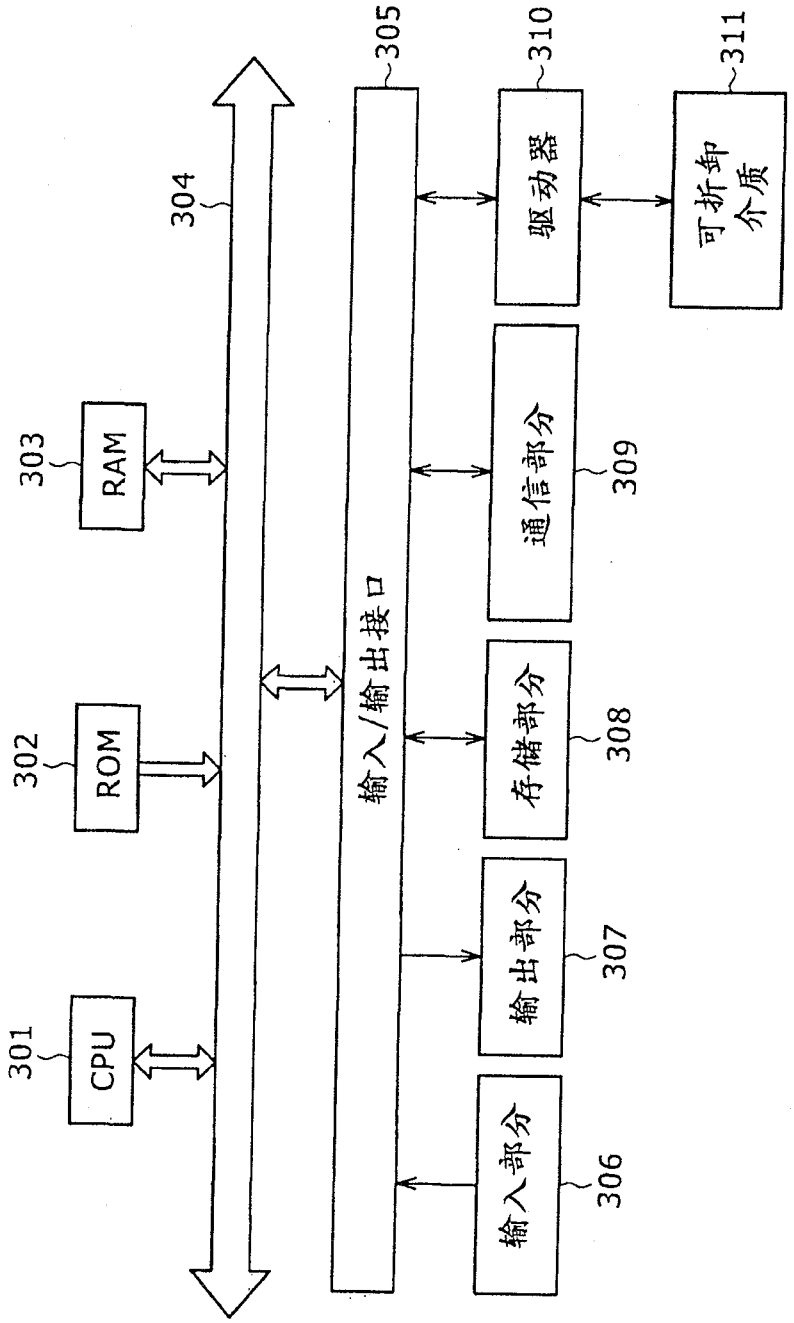

来自接收部分 232
LE密钥+密钥ID
211
当前 LE_Key ID
下一 LE_Key ID
142
143
LEKP表
密钥改变触发器产生部分
124
密钥改变触发器
123
密钥改变定时
145
帧复位
146
帧/线复位
150
元数据提取/分离部分
241
来自接收部分 231
101
密钥未发现信号
到状态呈现部分74,等等
元数据提取部分
233
31-D
LE_Key
Le_attribute_data
144
寄存器
125
Le_attribute_data
147
当前帧计数
148
寄存器
126
HD SDI的线数
149
AES输入产生部分
129
AES输入
32-D
31-D
LE_Key
144
解密部分
73
线复位
151
计数器
127
HD-SDI链路数
152
寄存器
128
帧/线复位
150
加密输入信号
102
到状态呈现部分74等等

图15


301
CPU
302
ROM
303
RAM
304
305
输入/输出接口
306
输入部分
307
输出部分
308
存储部分
309
通信部分
310
驱动器
311
可拆卸介质