[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/16 (2006.01)
H04N 7/167 (2006.01)

[12] 发明专利说明书

专利号 ZL 03806297.6

[45] 授权公告日 2008 年 4 月 9 日

[11] 授权公告号 CN 100380966C

[22] 申请日 2003.3.18 [21] 申请号 03806297.6

[30] 优先权

[32] 2002. 3.20 [33] JP [31] 078397/2002

[32] 2002.12.16 [33] JP [31] 364389/2002

[32] 2003. 2.28 [33] JP [31] 054134/2003

[86] 国际申请 PCT/JP2003/003232 2003.3.18

[87] 国际公布 WO2003/079689 英 2003.9.25

[85] 进入国家阶段日期 2004.9.17

[73] 专利权人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 小野贵敏 熊崎洋儿 山田茂
村上弘规 井上哲也 大森基司

[56] 参考文献

CN1284818A 2001.2.21

CN1255266A 2000.5.31

EP0866613A1 1998.9.23

CN1317204A 2001.10.10

EP1094667A1 2001.4.25

EBU REVIEW – TECHNICAL. EUROPEAN BROADCASTING UNION, 全文, FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM. 1995

武汉科技学院学报. 姚晓东等, 全文, 数字高清晰度电视条件接收系统实现方案探讨. 2000

审查员 夏 刊

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 程天正 罗 朋

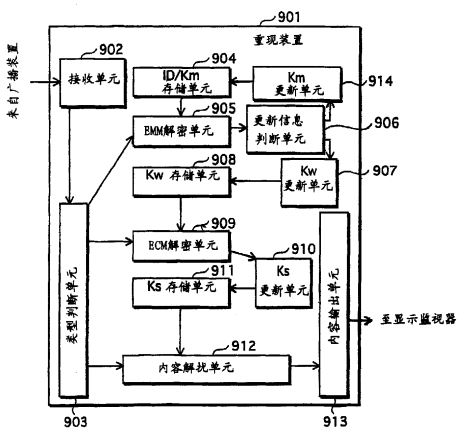
权利要求书 5 页 说明书 29 页 附图 26 页

[54] 发明名称

内容重现装置、方法以及密钥管理装置和系统

[57] 摘要

本发明提供一种可以防止用未授权的量现装置对内容进行非授权重现、而只使授权重现装置能够正确地重现内容的技术。 本发明的重现装置获得已经由第一密钥加密方法加密过的加密的密钥信息，并使用在存储单元中存储的密钥将加密过的密钥信息解密成密钥信息。 在解密后的密钥信息是解密密钥时，重现装置(i)获得已经被第二密钥加密方法加密过的加密的内容密钥，(ii)用解密密钥将加密过的内容密钥解密成内容密钥，(iii)获得已经被干扰加密方法加扰的加扰的内容，(iv)用解密后的内容密钥解扰加扰过的内容，和(v)重现解扰的内容。



1.一种内容重现装置，包含:

在其中存储着密钥的存储单元;

密钥信息解密单元，它能(i)获得已经由第一密钥加密方法加密过的加密的密钥信息，和(ii)用所述存储单元中存储的密钥将加密的密钥信息解密成密钥信息，该密钥信息或者是用于解密一个内容密钥的解密密钥，或者是用于更新所存储的密钥的密钥更新信息;

内容重现单元，它在解密后的密钥信息是解密密钥时，能(i)用解密密钥来解密已经被第二密钥加密方法加密过的一个加密的内容密钥，(ii)用解密后的内容密钥去解扰已经被一个干扰加密方法加扰过的一个加扰的内容，和(iii)重现解扰的内容; 以及

更新单元，它在解密后的密钥信息是密钥更新信息时，能按照密钥更新信息来更新所存储的密钥。

2.如权利要求1的内容重现装置，其中，

密钥信息有一个随附于它的标识符，用于将密钥信息标识为解密密钥或者密钥更新信息，并且

内容重现装置进一步包含

一个判断单元，它能按照标识符判断密钥信息究竟是解密密钥还是密钥更新信息。

3.如权利要求2的内容重现装置，其中，

密钥信息被包括在EMM中，EMM代表资格管理消息，并且

内容重现装置进一步包含

一个广播接收单元，它能接受包括已经用密钥加密了的经加密的EMM的广播数据，并由此获得加密过的密钥信息，并且

该密钥信息解密单元获得由广播接收单元接收的加密过的密钥信息。

4.如权利要求1的内容重现装置，其中，

更新单元通过根据对每个内容重现装置来说是独有的变换而生成新的密钥，从而来更新所存储的密钥。

5.如权利要求1的内容重现装置，其中，

更新单元通过根据对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的变换而生

成新的密钥，从而来更新所存储的密钥。

6.如权利要求1的内容重现装置，其中，

密钥更新信息包括要由其生成新的密钥的种子信息，并且

更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息转换成新的密钥而更新所存储的密钥。

7.如权利要求1的内容重现装置，其中，

密钥更新信息是指示密钥应当被更新的触发信息，并且

更新单元进一步包括:

发送子单元，它能响应触发信息而向管理一个或多个密钥的密钥管理装置发送请求信号以请求要由其生成新的密钥的种子信息;

种子信息接收子单元，它能接收密钥管理装置响应该请求信号而发送的种子信息，以及

更新单元通过按照在制造内容重现装置时确定的转换算法将所接收的种子信息转换成新的密钥而更新所存储的密钥。

8.如权利要求1的内容重现装置，其中，

密钥更新信息包括要由其生成新的密钥的种子信息，并且

更新单元进一步包括:

一个输出子单元，它能输出事件信息，该事件信息每次输出时是不同的，或者每隔一定的输出次数时是不同的，

更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息和事件信息转换成新的密钥而更新所存储的密钥，并且

内容重现装置进一步包含一个发送单元，它能向管理一个或多个密钥的密钥管理装置发送由输出子单元输出的事件信息。

9.如权利要求1的内容重现装置，其中，

在存储单元中存储的密钥对每个内容重现装置来说是独有的。

10.如权利要求1的内容重现装置，其中，

在存储单元中存储的密钥对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的。

11.如权利要求1的内容重现装置，还具有对每个内容重现装置来说是独有的ID，其中，

更新单元通过按照在制造内容重现装置时确定的转换算法将ID和种子信息转换成新的密钥而更新所存储的密钥，种子信息是要由其生

成新的密钥的信息。

12.如权利要求1的内容重现装置，还具有对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的ID，其中，

更新单元通过按照在制造内容重现装置时确定的转换算法将ID和种子信息转换成新的密钥而更新所存储的密钥，种子信息是要由其生成新的密钥的信息。

13. 用于内容重现装置的一种内容重现方法，该内容重现装置包括在其中存储着密钥的存储单元，该内容重现方法包含:

密钥信息解密步骤:(i)获得已经由第一密钥加密方法加密过的加密的密钥信息，和(ii)使用所述存储单元中存储的密钥将加密的密钥信息解密成密钥信息，该密钥信息或者是用于解密内容密钥的解密密钥，或者是用于更新所存储的密钥的密钥更新信息;

内容重现步骤:在解密的密钥信息是解密密钥时，(i)使用解密密钥来解密已经被第二密钥加密方法加密过的加密的内容密钥，(ii)使用解密的内容密钥解扰已经被干扰加密方法加扰过的加扰的内容，和(iii)重现解扰的内容;和

更新步骤:在解密的密钥信息是密钥更新信息时，按照密钥更新信息来更新所存储的密钥。

14.一种管理在密钥加密方法中所使用的管理密钥的密钥管理装置，包括:

密钥更新信息生成单元，它能生成用于更新所述管理密钥的密钥更新信息;

发送单元，它能使用所述管理密钥来加密密钥信息和向内容重现装置发送加密过的密钥信息，该密钥信息或是用于重现内容的解密密钥或是密钥更新信息;和

密钥更新单元，它能按照密钥更新信息来更新所述管理密钥。

15.如权利要求14的密钥管理装置，其中，

发送单元在发送密钥信息之前，向密钥信息附加一个用于将密钥信息标识为解密密钥或者密钥更新信息的标识符。

16.如权利要求15的密钥管理装置，其中，

密钥信息被包括在表示资格管理消息的EMM中，并且

发送单元通过广播向所述内容重现装置发送密钥信息。

17.如权利要求14的密钥管理装置，其中，

密钥更新信息包括要由其生成新的密钥的种子信息，并且

密钥更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息转换成新的密钥而更新所述管理密钥。

18.如权利要求14的密钥管理装置，其中，

密钥更新信息是指示所述管理密钥应当被更新的触发信息，并且

密钥更新单元进一步包括:

种子信息生成子单元，它能生成要由其生成新的密钥的种子信息；和

传送子单元，它能接收由已经获得触发信息的内容重现装置发送的请求信号，并响应该请求信号而向内容重现装置传送所生成的种子信息，并且

密钥更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息转换成新的密钥而更新所述管理密钥。

19.如权利要求14的密钥管理装置，其中，

密钥更新信息包括要由其生成新的密钥的种子信息，并且

密钥更新单元进一步包括

一个接收子单元，它能接收由已经获得种子信息的内容重现装置发送的事件信息，事件信息每次发送时是不同的，或者每隔一定的发送次数时是不同的，并且

密钥更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息和事件信息转换成新的密钥而更新所述管理密钥。

20.一种密钥管理系统，由(i)内容重现装置和(ii)密钥管理装置组成，该密钥管理装置管理在用于内容重现装置的密钥加密方法中使用的一个或多个密钥，该密钥管理系统包括:

包含在该密钥管理装置中的密钥更新信息生成单元，它能生成用于更新每个密钥的密钥更新信息;

包含在该密钥管理装置中的发送单元，它能用第一密钥来加密密钥信息和向内容重现装置发送加密过的密钥信息，该密钥信息或者是用于重现内容的解密密钥或者是密钥更新信息;

包含在该内容重现装置中的密钥信息解密单元，它能获得由发送

单元发送的加密的密钥信息，并用第二密钥将加密过的密钥信息解密成密钥信息，第二密钥存储在内容重现装置中；

包含在该密钥管理装置中的第一更新单元，它能按照密钥更新信息来更新第一密钥；和

包含在该内容重现装置中的第二更新单元，它在解密后的密钥信息是用于更新第二密钥的密钥更新信息时，能按照密钥更新信息来更新第二密钥。

内容重现装置、方法以及密钥管理装置和系统

技术领域

本发明涉及一种广播接收系统（以下称作“条件访问系统”），在该系统中只有被授权观看数字广播内容的用户所拥有的重现装置才能正确地重现内容，本发明特别涉及一种用于更新在重现内容时需要的主密钥的技术。

背景技术

在 MPEG-2 系统(ISO/IEC13818-1)中（这是一种标准的条件访问系统），发布者(distributor)将包括图像和声频的内容在用加扰密钥 Ks 加扰后进行发送。接收者在用加扰密钥 Ks 将该内容解扰后进行重现。这时，发布者和接受者各自需要有相同的加扰密钥 Ks。

发布者因此将加扰密钥 Ks 存储在一个称作 ECM(资格控制消息)的信息中，在用工作密钥 Kw 将它们加密后发送 ECM。此外，发布者还将工作密钥 Kw 存储在一个称作 EMM(资格管理消息)的信息中，在用对每个重现装置来说都是独有的主密钥 Km 将 EMM 加密后进行发送。

接收者用自己的主密钥 Km 解密 EMM，以获得工作密钥 Kw，然后用该工作密钥 Kw 来解密 ECM，以获得加扰密钥 Ks。这样，发布者和接受者就各自都有相同的加扰密钥 Ks。

图 1 表示条件访问系统的总体结构。

广播装置 101 通过广播向重现装置 102 多路传送和发送各种信息，其中包括加扰的内容、ECM 和 EMM。重现装置 102 解扰/解密该信息并在显示监视器 103 上显示之。这时，重现装置 102 用一个 ID 和一个存储在重现装置中的主密钥 Km 来进行解密，然后把加扰过的内容解扰。每个重现装置、每个制造商等等都按需要被分配以一个不同的 ID。每个重现装置、每个制造商等等也都按需要被分配以一个不同的主密钥 Km。主密钥与 ID 一一对应。

图 2 表示条件访问系统中的重现装置的结构。

在重现装置 201 中，接收单元 202 接收包括加扰的内容、ECM 和 EMM 的各种信息，而类型判断单元 203 则判断信息的类型。类型判断单元 203 视信息的类型而将信息传输到不同的单元。例如，它将加扰的

内容传输到内容解扰单元 211，将 ECM 传输到 ECM 解密单元 208，将 EMM 传输到 EMM 解密单元 205。

ID/Km 存储单元 204 存储重现装置 201 独有的 ID 和主密钥。EMM 解密单元 205 用主密钥 Km 解密 EMM，并向 Kw 更新单元 206 输入一个已经是解密的 EMM 的一部分的工作密钥 Kw。Kw 更新单元 206 从 EMM 解密单元 205 获得工作密钥 Kw 并更新现有的工作密钥 Kw。Kw 存储单元 207 存储已经被 Kw 更新单元 206 更新的工作密钥 Kw。

也有另一个例子，其中，为了更新现有的工作密钥，通过一个双向通信系统获得一个新的工作密钥。(例如，参看日本未审专利申请公开号 2002-16901)。

ECM 解密单元 208 用工作密钥 Kw 解密 ECM，并向 Ks 更新单元 209 输入一个已经解密的 ECM 的一部分的加扰密钥 Ks。Ks 更新单元 209 从 ECM 解密单元 208 获得加扰密钥 Ks 并更新现有的加扰密钥 Ks。

这里，工作密钥 Kw 和加扰密钥 Ks 的更新一般意味着覆写它们；然而，对工作密钥和加扰密钥增加内容也是可以接受的。

Ks 存储单元 210 存储已经被 Ks 更新单元 209 更新的加扰密钥 Ks。内容解扰单元 211 用加扰密钥 Ks 把加扰的内容解扰，并将解扰的内容输入到内容输出单元 212。内容输出单元 212 向显示监视器发送该内容。

图 3 表示条件访问系统中的重现装置的操作。

重现装置从广播装置接收 EMM（S301）。EMM 包括(i)要接收 EMM 的回访装置的 ID 和(ii)加密的工作密钥 E(Kw,Km)，这是用对应于该 ID 的主密钥 Km 所加密的工作密钥 Kw。这里和以下的 E(X,Y)表示“以密钥 Y 加密的信息 X”或者“以密钥 Y 加扰的信息 X”。

如果 EMM 中包含的 ID 与重现装置本身存储的 ID 相同，则重现装置就用重现装置自身中存储的 Km 解密 E(Kw,Km)。结果，重现装置获得工作密钥 Kw(S302)。

下一步，重现装置从广播装置接收 ECM(S303)。ECM 包括一个加密的加扰密钥 E(Ks,Kw)，这是用工作密钥 Kw 加密的加扰密钥 Ks。

重现装置用在重现装置自身中存储的工作密钥 Kw 解密 E(Ks,Kw)。结果，重现装置获得加扰密钥 Ks (S304)。

进一步，重现装置从广播装置接收加扰的内容 E(内容，

Ks)(S305)。

重现装置用在重现装置自身中存储加扰密钥 Ks 解扰 E(内容,Ks)。结果，重现装置获得内容(S306)，用户就能观看该内容。

图 4 表示其中有多个重现装置的条件访问系统的总体结构。

重现装置 1 和重现装置 2 接收从广播装置 101 发送的各种信息。图中省略了显示监视器。ID1 和 ID2 被分别分配给每一个重现装置，并且彼此不同。由于 ID 于主密钥 Km 是一一对应的，Km1 和 Km2 也彼此不同。这里，将不同的 ID 分配给每个重现装置，但是将不同的 ID 分配给每个制造商、每个型号的重现装置、每个生产批次(production lot)或者每个特定的组，那也是可以接受的。在这些情况下，一个组内的多个重现装置具有相同的 ID 和相同的主密钥 Km，但是这些 ID 和主密钥 Km 与另一组内的重现装置所拥有的 ID 和主密钥 Km 是不同的。

图 5 表示在条件访问系统中多个重现装置的操作。

重现装置 1 选择性地从广播装置接收 EMM1（S501）。EMM1 包括 ID1 和加密的工作密钥 E(Kw,Km1)，这是用对应于 ID1 的主密钥 Km1 加密的工作密钥 Kw。因为 EMM1 中包括 ID1，所以，重现装置 1 能确定这个特定的 EMM 集的目的地是重现装置 1 自己。

重现装置 1 用重现装置 1 自身中存储的 Km1 解密 E(Kw,Km1)。结果，重现装置 1 获得工作密钥 Kw(S502)。

重现装置 2 选择性地从广播装置接收 EMM2（S503）。EMM2 包括 ID2 和加密的工作密钥 E(Kw,Km2)，这是用对应于 ID2 的主密钥 Km2 加密的工作密钥 Kw。因为 EMM2 中包括 ID2，所以，重现装置 2 能确定这个特定的 EMM 集的目的地是重现装置 2 自己。

重现装置 2 用重现装置 2 自身中存储的 Km2 解密 E(Kw,Km2)。结果，重现装置 2 获得工作密钥 Kw(S504)。

重现装置 1 和重现装置 2 就是这样获得各自的工作密钥 Kw 的。此后的过程与图 3 中相同，因此将省略对其的解释。

以下说明一种防止可能存在的未授权(unauthorized)装置重现内容的方法。

图 6 表示其中有非授权装置的条件访问系统的总体结构。

未授权重现装置是把自己伪装成具有 ID2 和已经以非授权方式获得的主密钥 Km2 的重现装置 2。在这种情况下，非授权装置能够假装成

它是重现装置 2，并按图 5 中所示的相同程序重现内容。

在这个方法中，当已知存在一个未授权装置时，广播装置就不发送包括 ID2 的 EMM，这样就有可能防止非授权重现内容。

图 7 表示在防止非授权装置进行对内容的非授权重现时重现装置的操作。

图 7 与图 5 的区别在于，广播装置只发送用于重现装置 1 的 EMM1(S501)，而不发送用于重现装置 2 的 EMM2。这样，非授权装置就不能获得工作密钥 Kw。结果，非授权装置就不能获得加扰密钥 Ks(S701)，也就不能接收内容(702)。

然而这个方法有一个问题。由于广播装置不发送包括 ID2 的 EMM，作为授权装置的重现装置 2 将也不能重现内容。

因此，本发明的第一个目的是提供一种技术，它有可能防止未授权的重现装置进行内容重现，而只让授权重现装置能正确地重现内容。

本发明的第二个目的是提供一种技术，它通过利用内容被发送时所经过的通道来只让授权重现装置能正确地重现内容。

发明内容

本发明提供一种内容重现装置，包含：在其中存储有密钥的存储单元；密钥信息解密单元，它能(i)获得已经由第一密钥加密方法加密的加密过的密钥信息，和(ii)用所述存储单元中存储的密钥将加密过的密钥信息解密成密钥信息，该密钥信息或者是用于解密一个内容密钥的解密密钥，或者是用于更新所存储的密钥的密钥更新信息；内容重现单元，它在解密过的密钥信息是解密密钥时，能(i)用解密密钥把已经被第二密钥加密方法加密的加密的内容密钥解密，(ii)用解密过的内容密钥把已经被干扰加密方法加扰的加扰的内容解扰，和(iii)重现解扰过的内容；以及更新单元，它在解密过的密钥信息是密钥更新信息时，能按照密钥更新信息来更新所存储的密钥。

有了这个安排，内容重现装置获得密钥信息，并且(a)当解密的密钥信息是密钥更新信息时，更新密钥；和(b)当密钥信息是解密密钥时，用解密密钥重现内容。通过以这种方式按照密钥更新信息来更新密钥，当获得已经用更新的密钥加密了的密钥信息时，内容重现装置将能正确地解密这个加密过的密钥信息。

于是，在密钥被更新之后，只有授权的内容重现装置才能重现内容，因此就有可能防止未授权的重现装置进行内容重现。

内容重现装置可以有一种安排，其中，密钥信息有一个随附的标识符，用于将密钥信息标识为解密密钥或者密钥更新信息，并且内容重现装置进一步包含一个判断单元，它能按照标识符判断密钥信息是解密密钥还是密钥更新信息。

有了这个安排，内容重现装置就能根据标识符判断密钥信息是解密密钥还是密钥更新信息。

内容重现装置可以有一种安排，其中，密钥信息被包括在 EMM 即资格管理消息中，并且内容重现装置进一步包含一个广播接收单元，它能接受包括已经被用密钥加密了的加密的 EMM 的广播数据并由此获得加密的密钥信息，密钥信息解密单元获得由广播接收单元接收的加密的密钥信息。

更新密钥的方法之一是，密钥的管理者向每个授权用户发送一个其上记录有新的密钥的便携式介质。在这个方法中，每个授权用户需要很多天才能接收到便携式介质，在此期间授权用户有可能丧失观看内容的特权。同时，从密钥管理者的角度来看，当多个内容重现装置的密钥需要更新时就有必要向每个用户发送便携式介质，管理者要承担的成本很高。

然而，有了上述的安排，内容重现装置就能通过接收广播数据来获得密钥更新信息。由于密钥更新信息是通过广播发送的，就有可能迅速地更新密钥。

这样，授权用户将不会丧失上述的特权。此外，还有可能通过用广播传送密钥更新信息而同时地把对密钥的更新通知多个内容重现装置。

这样，密钥的管理者就能降低上述的成本。

内容重现装置可以有一种安排，其中，更新单元通过根据对每个内容重现装置来说是独有的变换而生成新的密钥，从而来更新所存储的密钥。

内容重现装置可以有一种安排，其中，更新单元通过根据对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的变换而生成新的密钥，从而来更新所存

储的密钥。

有了这个安排，由于密钥是根据对每个内容重现装置来说是独有的变换而更新的，或者是根据对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的变换而更新的，即使内容重现装置经过了反向工程(reverse-engineered)且密钥的转换方法被泄密，也只有有限数量的内容重现装置是需要对其采取措施的。

内容重现装置可以有一种安排，其中，密钥更新信息包括要由其生成新的密钥的种子信息，并且更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息转换成新的密钥而更新所存储的密钥。

有了这个安排，由于密钥更新信息包括种子信息，内容重现装置就能获得种子信息并通过转换种子信息而生成新的密钥。

内容重现装置可以有一种安排，其中，密钥更新信息是指示密钥应当被更新的触发(trigger)信息，更新单元进一步包括：发送子单元，它能响应触发信息而向管理一个或多个密钥的密钥管理装置发送请求要由其生成新的密钥的种子信息的请求信号；种子信息接收子单元，它能接收密钥管理装置响应该请求信号而发送的种子信息，以及更新单元通过按照在制造内容重现装置时确定的转换算法将所接收的种子信息转换成新的密钥而更新所存储的密钥。

有了这个安排，内容重现装置获得触发信息并由于该触发信息而认识到密钥需要被更新。然后，内容重现装置向密钥管理装置发送对种子信息的请求，接收种子信息，并通过转换种子信息而获得新的密钥。在接收密钥更新信息之后与密钥管理装置通信具有如下两个优点：

第一个优点是，密钥管理装置能够判定已经从哪个内容重现装置衍生出了未授权重现装置。例如，如果已经做出了使得内容重现装置需要发送它们自己的ID作为请求信号的安排，而且存在未授权重现装置，则同一个ID将被多于一次地发送到密钥管理装置。于是，密钥管理装置就能判定具有这个特定ID的内容重现装置就是那个衍生出了未授权重现装置的内容重现装置。

第二个优点是，密钥管理装置能够发现内容重现装置正在更新主

密钥。例如，在只通过广播发送种子信息的情况下，密钥管理装置不能发现内容重现装置正在更新主密钥。然而，有了上述安排，密钥管理装置就能证实至少内容重现装置已经接收到密钥更新信息，因为存在着来自内容重现装置的通信。

内容重现装置可以有一种安排，其中，密钥更新信息包括要由其生成新的密钥的种子信息，并且更新单元进一步包括一个输出子单元，它能输出事件信息，该事件信息每次输出时不同，或者每隔一定的输出次数时不同，更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息和事件信息转换成新的密钥而更新所存储的密钥，且内容重现装置进一步包含一个发送单元，它能向管理一个或多个密钥的密钥管理装置发送由输出子单元输出的事件信息。

有了这个安排，内容重现装置从种子信息和事件信息中生成新的密钥，并且也发送事件信息，以便让密钥管理装置有相同的新密钥。在接收密钥更新信息之后与密钥管理装置通信具有如下两个优点：

第一个优点是，密钥管理装置能够判定已经从哪个内容重现装置衍生出了未授权重现装置。例如，如果已经做出了使得内容重现装置需要发送它们自己的 ID 作为请求信号的安排，而且存在未授权的重现装置，则同一个 ID 将被多于一次地发送到密钥管理装置。于是，密钥管理装置就能判定具有这个特定 ID 的内容重现装置就是那个其衍生出了未授权重现装置的内容重现装置。

第二个优点是，密钥管理装置能够发现内容重现装置正在更新主密钥。例如，在只通过广播发送种子信息的情况下，密钥管理装置不能发现内容重现装置正在更新主密钥。然而，有了上述安排，密钥管理装置就能证实至少内容重现装置已经接收到密钥更新信息，因为有来自内容重现装置的通信。

内容重现装置可以有一种安排，其中，在存储单元中存储的密钥对每个内容重现装置来说是独有的。

内容重现装置可以有一种安排，其中，在存储单元中存储的密钥对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的。

有了这个安排，由于密钥对每个内容重现装置来说是独有的，或者是对内容重现装置的每个生产批次、内容重现装置的每个型号或者

内容重现装置的每个制造商来说是独有的，即使内容重现装置经过了反向工程且密钥的转换方法被泄密，也只有有限数量的内容重现装置是需要对其采取措施的。

内容重现装置可以进一步有对每个内容重现装置来说是独有的ID，其中，更新单元通过按照在制造内容重现装置时确定的转换算法将ID和种子信息转换成新的密钥而更新所存储的密钥，种子信息是要由其生成信息的密钥的信息。

内容重现装置可以进一步有对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的ID，其中，更新单元通过按照在制造内容重现装置时确定的转换算法将ID和种子信息转换成新的密钥而更新所存储的密钥，种子信息是要由其生成信息的密钥的信息。

有了这个安排，由于ID对每个内容重现装置来说是独有的，或者是对内容重现装置的每个生产批次、内容重现装置的每个型号或者内容重现装置的每个制造商来说是独有的，即使内容重现装置经过了反向工程且密钥的转换方法被泄密，也只有有限数量的内容重现装置是需要对其采取措施的。

本发明进一步提供一种用于包括在其中存储有密钥的存储单元的内容重现装置的内容重现方法，该内容重现方法包含：密钥信息解密步骤，即(i)获得已经由第一密钥加密方法加密的经加密的密钥信息，和(ii)用所述存储单元中存储的密钥将加密的密钥信息解密成密钥信息，该密钥信息或者是用于解密内容密钥的解密密钥，或者是用于更新所存储的密钥的密钥更新信息；内容重现步骤，即在解密的密钥信息是解密密钥时，(i)用解密密钥解密已经被第二密钥加密方法加密的经加密的内容密钥，(ii)用解密的内容密钥解扰已经被干扰加密方法加扰的加扰的内容，和(iii)重现解扰的内容；以及更新步骤，即在解密的密钥信息是密钥更新信息时，按照密钥更新信息来更新所存储的密钥。

有了这个安排，内容重现装置获得密钥信息，并且(a)当解密的密钥信息是密钥更新信息时，更新密钥；和(b)当密钥信息是解密密钥时，用解密密钥重现内容。通过以这种方式按照密钥更新信息来更新密钥，当获得已经用更新的密钥加密了的密钥信息时，内容重现装置

将能正确地解密这个加密的密钥信息。

于是，在密钥被更新之后，只有授权的内容重现装置才能重现内容，因此就有可能防止未授权的重现装置进行内容重现。

本发明进一步提供一种指示计算机重现内容的程序，该计算机包括在其中存储有密钥的存储单元，该程序包含：密钥信息解密步骤，即(i)获得已经由第一密钥加密方法加密的加密的密钥信息，和(ii)用所存储的密钥将加密的密钥信息解密成密钥信息，该密钥信息或者是用于解密内容密钥的解密密钥，或者是用于更新该密钥的密钥更新信息；内容重现步骤，即在解密的密钥信息是解密密钥时，(i)用解密密钥解密已经被第二密钥加密方法加密的加密的内容密钥，(ii)用解密的内容密钥解扰已经被干扰加密方法加扰的加扰的内容，和(iii)重现解扰的内容；以及更新步骤，即在解密的密钥信息是密钥更新信息时，按照密钥更新信息来更新密钥。

有了这个安排，计算机获得密钥信息，并且(a)当解密的密钥信息是密钥更新信息时，更新密钥；和(b)当密钥信息是解密密钥时，用解密密钥重现内容。通过以这种方式按照密钥更新信息来更新密钥，当获得已经用更新的密钥加密了的密钥信息时，内容重现装置将能正确地解密这个加密的密钥信息。

于是，在密钥被更新之后，只有授权的内容重现装置才能重现内容，因此就有可能防止未授权的重现装置进行内容重现。

本发明进一步提供管理在密钥加密方法中使用的管理密钥的密钥管理装置，包含：密钥更新信息生成单元，它能生成用于更新所述管理密钥的密钥更新信息；发送单元，它能用所述管理密钥来加密密钥信息和向重现装置发送加密的密钥信息，密钥信息是用于重现内容的解密密钥或者是密钥更新信息；和密钥更新单元，它能按照密钥更新信息更新所述管理密钥。

有了这个安排，由于密钥管理装置发送加密的密钥信息给内容重现装置，密钥管理装置和内容重现装置各自将能够有相同的密钥信息。密钥管理装置也能够按照包含在密钥信息中的密钥更新信息来更新密钥。因此，在密钥被更新之后，只有授权的内容重现装置才能重现内容，因此有可能防止非授权的内容重现装置进行内容重现。

密钥管理装置可以有一种安排，其中，发送单元在发送密钥信息

之前，向密钥信息附加一个用于识别密钥信息为解密密钥还是密钥更新信息的标识符。

有了这个安排，密钥管理装置就能以一种形式发送诸如解密密钥和密钥更新信息的两种信息。

密钥管理装置可以有一种安排，其中，密钥信息被包括在 EMM 即资格管理消息中，并且发送单元通过广播向所述内容重现装置发送密钥信息。

有了这个安排，密钥管理装置能通过广播发送密钥更新信息。由于密钥更新信息是通过广播发送的，就有可能迅速地更新密钥。

密钥管理装置可以有一种安排，其中，密钥更新信息包括要由其生成新的密钥的种子信息，并且密钥更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息转换成新的密钥而更新所述管理密钥。

有了这个安排，由于密钥更新信息包括种子信息，密钥管理装置就能生成种子信息并也能通过转换种子信息而生成新的密钥。

密钥管理装置可以有一种安排，其中，密钥更新信息是指示管理密钥应当被更新的触发信息，密钥更新单元进一步包括：种子信息生成子单元，它能生成要由其生成新的密钥的种子信息；传送子单元，它能接收由已经获得触发信息的内容重现装置发送的请求信号，并响应该请求信号而向内容重现装置传送生成的种子信息，并且密钥更新单元通过按照在制造内容重现装置时确定的转换算法将所接收的种子信息转换成新的密钥而更新所述管理密钥。

有了这个安排，密钥管理装置生成触发信息并用触发信息通知内容重现装置密钥需要被更新。然后，密钥管理装置从内容重现装置接收请求种子信息的请求信号，响应该请求信号而向内容重现装置发送种子信息，并通过转换种子信息而获得新的密钥。在发送密钥更新信息之后与内容重现装置通信具有如下两个优点：

第一个优点是，密钥管理装置能够判定已经从哪个内容重现装置衍生出了未授权的重现装置。例如，如果已经做出了使得内容重现装置需要发送它们自己的 ID 作为请求信号的安排，而且存在未授权的重现装置，则同一个 ID 将被多于一次地发送到密钥管理装置。于是，密钥管理装置就能判定具有这个特定 ID 的内容重现装置就是从其衍生出

了未授权重现装置的内容重现装置。

第二个优点是，密钥管理装置能够发现内容重现装置正在更新主密钥。例如，在只通过广播发送种子信息的情况下，密钥管理装置不能发现内容重现装置正在更新主密钥。然而，有了上述安排，密钥管理装置就能证实至少内容重现装置已经接收到密钥更新信息，因为有来自内容重现装置的通信。

密钥管理装置可以有一种安排，其中，密钥更新信息包括要由其生成新的密钥的种子信息，并且密钥更新单元进一步包括一个接收子单元，它能接收由已经获得种子信息的内容重现装置发送的事件信息，事件信息每次发送时不同，或者每隔一定的发送次数时不同，并且密钥更新单元通过按照在制造内容重现装置时确定的转换算法将种子信息和事件信息转换成新的密钥而更新所述管理密钥。

有了这个安排，密钥管理装置从内容重现装置接收事件信息并从种子信息和事件信息中生成新的密钥。在发送密钥更新信息之后与内容重现装置通信具有如下两个优点：

第一个优点是，密钥管理装置能够判定已经从哪个内容重现装置衍生出了未授权的重现装置。例如，如果已经做出了使得内容重现装置需要发送它们自己的 ID 作为请求信号的安排，而且存在未授权重现装置，则同一个 ID 将被多于一次地发送到密钥管理装置。于是，密钥管理装置就能判定具有这个特定 ID 的内容重现装置就是从其衍生出了未授权的重现装置的内容重现装置。

第二个优点是，密钥管理装置能够发现内容重现装置正在更新主密钥。例如，在只通过广播发送种子信息的情况下，密钥管理装置不能发现内容重现装置正在更新主密钥。然而，有了上述安排，密钥管理装置就能证实至少内容重现装置已经接收到密钥更新信息，因为存在着来自内容重现装置的通信。

本发明进一步提供一种密钥管理系统，其组成是(i)内容重现装置，和(ii)管理在内容重现装置的密钥加密方法中使用的一个或多个密钥的密钥管理装置，密钥管理系统包含：包含在密钥管理装置中的密钥更新信息生成单元，它能生成用于更新每个密钥的密钥更新信息；包含在密钥管理装置中的发送单元，它能用第一密钥来加密密钥信息和向内容重现装置发送加密的密钥信息，密钥信息是用于重现内

容的解密密钥或者是密钥更新信息；包含在内容重现装置中的密钥信息解密单元，它能获得由发送单元发送的加密的密钥信息，用第二密钥将加密的密钥信息解密成密钥信息，第二密钥存储在内容重现装置中；包含在密钥管理装置中的第一更新单元，能按照密钥更新信息来更新第一密钥；和包含在内容重现装置中的第二更新单元，它在解密的密钥信息是用于更新第二密钥的密钥更新信息时，按照密钥更新信息来更新第二密钥。

有了这个安排，内容重现装置和密钥管理装置各自获得密钥信息，并且(a)当密钥信息是密钥更新信息时，更新密钥；和(b)当密钥信息是解密密钥时，用解密密钥重现内容。通过以这种方式按照密钥更新信息来更新密钥，当获得已经用更新的密钥加密了的密钥信息时，内容重现装置和密钥管理装置各自都将能正确地解密这个加密的密钥信息。

于是，在密钥被更新之后，只有授权的内容重现装置才能重现内容，因此就有可能防止未授权的重现装置进行内容重现。

附图说明

图 1 表示条件访问系统的总体结构；

图 2 表示条件访问系统中的重现装置的结构；

图 3 表示条件访问系统中的重现装置的操作；

图 4 表示其中有多个重现装置的条件访问系统的总体结构；

图 5 表示其中有多个重现装置的条件访问系统的操作；

图 6 表示其中有非授权装置的条件访问系统的总体结构；

图 7 表示在防止非授权装置进行对内容的非授权重现时重现装置的操作；

图 8 表示第一个实施例的条件访问系统的总体结构；

图 9 表示第一个实施例的条件访问系统中的重现装置的结构；

图 10 表示第一实施例中的 Km 更新单元的详细结构；

图 11 表示标准 EMM 的数据结构；

图 12 表示用于更新主密钥 Km 的 EMM 的数据结构；

图 13A 和 13B 表示在 Km 生成单元中使用的算法的例子；

图 14 表示条件访问系统中的重现装置的操作；

图 15 表示条件访问系统中的密钥管理装置的结构；

图 16 表示由密钥管理装置管理 ID 和主密钥 Km 的例子;

图 17 表示条件访问系统中的密钥管理装置的操作;

图 18 表示重现装置在防止非授权装置非授权观看内容时的操作;

图 19 表示第二实施例的条件访问系统的总体结构;

图 20 表示第二实施例中 Km 更新单元的详细结构;

图 21 表示用于更新主密钥 Km 的 EMM 的数据结构;

图 22 表示条件访问系统中的密钥管理装置的结构;

图 23 表示第三实施例的条件访问系统的总体结构;

图 24 表示第三实施例中 Km 更新单元的详细结构;

图 25 表示条件访问系统中的密钥管理装置的结构; 以及

图 26 表示 DVD 重现装置的结构。

实施本发明的最佳方式

第一实施例

条件访问系统的总体结构

图 8 表示第一实施例的条件访问系统的总体结构。

第一实施例的条件访问系统包含密钥管理装置 801、制造机器 802、重现装置 803 和广播装置 804。

首先, 解释密钥管理装置 801 和重现装置 803 各自如何获得相同的 ID 和相同的主密钥 Km。

密钥管理装置 801 为制造机器 802 分配一个 ID 和一个主密钥, ID 和主密钥按照需要对每个重现装置、每个生产批次、每个型号或者每个制造商来说是独有的。

制造重现装置 803 的制造机器 802 将已经由密钥管理装置 801 分配的 ID 和主密钥 Km 装配到重现装置 803 中, 然后为用户提供重现装置 803。

这样, 密钥管理装置 801 和重现装置 803 各自获得相同的 ID 和相同的主密钥 Km。

第二, 解释用户观看所需内容所遵守的程序。这里, 假设例如用户的重现装置 803 中存储有 ID“00000001”和主密钥 Km“27832529”。

用户向广播所需内容的广播装置 804 发出一个观看内容的请求。此时, 用户通知广播装置 804: 在其重现装置 803 中存储 ID“00000001”。

广播装置 804 接收来自用户的请求，将 ID“00000001”和该重现装置 803 的工作密钥 Kw 存储到 EMM 中，将该 EMM 发送到密钥管理装置 801。

这里，工作密钥 Kw 是一个只有被授权观看内容的用户所拥有的重现装置才能获得的密钥。

密钥管理装置 801 从广播装置 804 接收 EMM，并提取存储在 EMM 中的 ID“00000001”。然后，密钥管理装置 801 确认主密钥 Km“27832529”对应于这个 ID，并用主密钥 Km“27832529”加密 EMM，然后将 EMM 发送给广播装置 804。

广播装置 804 广播加密的 EMM。

重现装置 803 选择性地接收 EMM，根据 EMM 中存储的 ID 判定该特定的 EMM 集是以该重现装置本身为目的地的。在本例中，EMM 中存储的 ID 是“00000001”，因此重现装置 803 判定该 EMM 集是以重现装置 803 自己为目的地的。随后，重现装置 803 用主密钥“27852529”解密 EMM，获得工作密钥 Kw。

这就是广播装置 804 和重现装置 803 各自如何获得相同的工作密钥 Kw。

除了 EMM 外，广播装置 804 也广播包括加扰密钥 Ks 的 ECM 以及用加扰密钥 Ks 加扰的内容。重现装置 804 也能通过用工作密钥 Kw 解密 ECM 而获得加扰密钥 Ks，并能通过解扰已经被加扰密钥 Ks 加扰的加扰的内容而获得内容。

以下解释主密钥 Km 的更新，这是本实施例的特征之一。

主密钥原则上不需要被更新。然而，如果重现装置 803 的 ID“00000001”和主密钥 Km“27832529”被泄漏给例如非授权用户，则该非授权用户通过复制并将这些 ID 和主密钥 Km 登录入其重现装置，就能够以非授权方式观看重现装置 803 的用户已经被授权观看的内容。在这种情况下，就有必要更新主密钥 Km。

因此，广播装置 804 在 EMM 中存储(i)需要更新主密钥的重现装置的 ID 和(ii)要由其生成新的主密钥的种子信息，然后广播 EMM。然后，需要更新主密钥的重现装置根据种子信息生成新的主密钥。

这里，用来根据种子信息生成新密钥的算法，在制造重现装置时被确定，并以可靠的方式安装在重现装置中。同样的算法也被可靠地安装在密钥管理装置中。这意味着，由于只有授权用户的密钥管理装

置和重现装置存储相同的算法，所以只有授权用户的密钥管理装置和重现装置才能有相同的新主密钥。

因此，本实施例的条件访问系统能够在主密钥被更新后防止非授权用户进行非授权的观看。

以下详细解释用来实现这种条件访问系统的重现装置和密钥管理装置。

重现装置的结构

图 9 表示条件访问系统中的重现装置的结构。

重现装置 901 包含接收单元 902、类型判断单元 903、ID/Km 存储单元 904、EMM 解密单元 905、更新信息判断单元 906、Kw 更新单元 907、Kw 存储单元 908、ECM 解密单元 909、Ks 更新单元 910、Ks 存储单元 911、内容解扰单元 912、内容输出单元 913 和 Km 更新单元 914。

接收单元 902 从广播装置接收包括加扰的内容、ECM 和 EMM 等各种信息。

类型判断单元 903 根据信息的类型将信息传送到不同的单元，例如，它将加扰的内容传送到内容解扰单元 912，将 ECM 传送到 ECM 解密单元 909、将 EMM 传送到 EMM 解密单元 905。

ID/Km 存储单元 904 存储重现装置 901 独有的 ID 和主密钥，并根据需要将主密钥 Km 输入到 EMM。主密钥 Km 的初始值是已经被制造商安装在重现装置中的值，并根据需要被 Km 更新单元 914 更新。

EMM 解密单元 905 用主密钥 Km 解密 EMM 并将解密的 EMM 输入到更新信息判断单元 906。

更新信息判断单元 906 按照 EMM 中包含的标识符判断 EMM 存储的是用于更新主密钥 Km 的种子信息还是用于更新工作密钥的新工作密钥。标识符将在以后作解释。

如果存储的是工作密钥 Kw，更新信息判断单元 906 将该工作密钥 Kw 输入到 Kw 更新单元 907。如果存储的是种子信息，更新信息判断单元 906 将该种子信息输入到 Km 更新单元 914。

Kw 更新单元 907 从更新信息判断单元 906 获得工作密钥 Kw 并更新现有的工作密钥。工作密钥一般是通过覆写而更新的，然而，通过增加内容而更新工作密钥也是可以接受的。

Kw 存储单元 908 存储由 Kw 更新单元 907 更新的工作密钥 Kw，并

根据需要将工作密钥 Kw 输入到 ECM 解密单元 909。

ECM 解密单元 909 用工作密钥解密 ECM，并将存储在 ECM 中的新的加扰密钥 Ks 输入到 Ks 更新单元 910。

Ks 更新单元 910 从 ECM 解密单元 909 获得加扰密钥 Ks，并更新现有的加扰密钥 Ks。加扰密钥一般是通过覆写而更新的，然而，通过对其增加内容而更新加扰密钥也是可以接受的。

Ks 存储单元 911 存储由 Ks 更新单元 910 更新的加扰密钥 Ks，并根据需要将加扰密钥 Ks 输入到内容解扰单元 912。

内容解扰单元 912 用加扰密钥 Ks 来解扰已加扰的内容，并将解扰的内容输入到内容输出单元 913。

内容输出单元 913 把内容发送到显示监视器。

Km 更新单元 914 从更新信息判断单元 906 获得种子信息，用种子信息更新主密钥 Km。主密钥一般是通过覆写而更新的，然而，通过对其增加内容而更新主密钥也是可以接受的。如果是向主密钥增加内容，ID/Km 存储单元 904 将能够存储在更新之前就有的所有主密钥以及当前的主密钥。因此，如果当前主密钥由于出错而不能使用，就有可能转而使用更新之前的主密钥之一。如果 ID/Km 存储单元 904 除存储当前主密钥外只存储初始的主密钥，那也是可以接受的。

此外，同时更新主密钥和 ID 也是可以接受的。用 ID 的一部分作为生成数并更新 ID 与主密钥的组合的生成，也是可以接受的。在这种情况下，ID 可以通过覆写或者通过对其增加内容而被更新。

图 10 表示第一实施例中的 Km 更新单元的详细结构。

Km 更新单元 914 包含种子信息获得单元 1001、Km 生成单元 1002 和 Km 保留单元 1003。

种子信息获得单元 1001 从更新信息判断单元获得种子信息，将种子信息输入到 Km 生成单元 1002，以作为用于生成主密钥的算法中的变量。

Km 生成单元 1002 用已经安装在 Km 生成单元 1002 自身中的算法生成新的主密钥 Km′。该算法对每个重现装置、每个生产批次、每个型号或每个制造商来说是唯一的。相同的算法也被存储在密钥管理装置中。

Km 保留单元 1003 以 ID/Km 存储单元 904 能够存储的形式保留主

密钥 Km。

这样，重现装置 901 就能用从广播装置广播的 EMM 更新主密钥。

如下所述，根据新的主密钥是在哪个时刻被生成的，Km 更新单元 914 有两种可能性，并且可以是任何一种可能性。

第一种可能是，一旦获得种子信息，就生成新的主密钥。

第二种可能是，获得种子信息后将其存储起来，直到需要生成新的主密钥。在这种情况下，例如可以在 EMM 被输入到 EMM 解密单元并收到从 EMM 解密单元发送的信号之后生成新的主密钥。

以下解释 EMM 的数据结构。

图 11 表示标准的 EMM 的数据结构。

EMM 由 ID 段和数据段组成。ID 段存储要接收该特定 EMM 集的重现装置的 ID。重现装置因此能在从广播装置广播的不同 EMM 集中选择性地只解密其中存储该重现装置的 ID 的 EMM。

数据段存储标识符和密钥信息。标识符标识存储在数据段中的密钥信息是工作密钥还是种子信息。例如，可以安排得使得如果标识符是"0x01"，则存储的是工作密钥，如果标识符是"0x02"，则存储的是种子信息。

数据段也存储其它信息，诸如信息长度、协议号码、到期日期，不过对这些事项的解释将被省略。

图 12 表示用于更新主密钥的 EMM 的数据结构。

用于更新主密钥的 EMM 集同标准 EMM 一样也是由 ID 段和数据段组成的。数据段存储标识符和种子信息。种子信息是要由其生成信息的主密钥的信息，例如主密钥的生成数、随机数或它们的组合。

图 13A 和 13B 表示在 Km 生成单元中使用的算法的例子。

图 13A 指出一种运用原始哈希函数(original hash function)根据重现装置的 ID 和生成数获得主密钥的方法。

图 13B 指出一种运用原始加密函数(original encrypting function)通过加密在密钥管理装置中生成的随机数而获得主密钥的方法。

只要重现装置和密钥管理装置都能各自安全地拥有新的主密钥，生成新的主密钥的方法就不仅限于这里所提及的方法。例如，通过将 ID、生成数和种子信息输入到每个制造商独有的的原始哈希函数中来

生成新的主密钥，这就是可以接受的。

重现装置的操作

图 14 表示条件访问系统中重现装置的操作。

重现装置从广播装置接收包括加扰的内容、ECM 和 EMM 等各种信息。以下解释仅针对接收 EMM 的情形。

当重现装置接收 EMM 时，它根据 EMM 中存储的标识符来判断 EMM 中包含的是工作密钥还是种子信息（S1401）。

如果 EMM 中包含种子信息(S1402,Y)，则重现装置获得包含在 EMM 中的种子信息(S1403)。

重现装置然后从种子信息生成新的主密钥(S1404)。

重现装置存储在步骤 S1404 中生成的主密钥并从下一个时机开始使用它(S1405)。

如果在步骤 S1402EMM 中包含工作密钥(S1402,N)，则重现装置获得工作密钥(S1406)。

重现装置存储在步骤 S1406 中解密的工作密钥,以便能在接收 ECM 的下一个时机开始使用之(S1407)。

至此，对能够从 EMM 中存储的种子信息生成新的主密钥的重现装置的操作和结构作了解释。以下解释密钥管理装置如何能与重现装置有相同的新的主密钥。

密钥管理装置的结构

图 15 表示条件访问系统中密钥管理装置的结构。

密钥管理装置 1501 包含 EMM 接收单元 1502、密钥更新判断单元 1503、种子信息生成和插入单元 1504、Km 更新单元 1505、ID/Km 存储单元 1506、EMM 加密单元 1507 和加密 EMM 发送单元 1508。

EMM 接收单元 1502 接收从广播装置发送的 EMM 并将 EMM 输入到密钥更新判断单元 1503。

密钥更新判断单元 1503 判断 EMM 是否包含表明主密钥需要被更新的某种信息。更具体来说，如果安排得使得标识符"0x02"表示"需要更新主密钥"，则密钥更新判断单元 1503 检查标识符是不是"0x02"。如果标识符是"0x02"，则密钥更新判断单元将该事实通知种子信息生成和插入单元 1504。EMM 将被输入到 EMM 加密单元 1507。

种子信息生成和插入单元 1504 从密钥更新判断单元 1503 接收通

知，生成种子信息，将其插入 EMM 中，并且还把种子信息输入到 Km 更新单元 1505。种子信息是要由其生成新的主密钥的信息，例如可以是主密钥的生成数或者随机数。

Km 更新单元 1505 从种子信息生成和插入单元 1504 获得种子信息，并用种子信息更新主密钥 Km。这里，被用来由种子信息生成新的主密钥的算法也被存储在重现装置中。

ID/Km 存储单元 1506 存储每个重现装置、每个生产批次、每个型号或制造商的唯一性的 ID 和主密钥，并根据需要将主密钥 Km 输入到 EMM 加密单元 1507。主密钥 Km 的初始值是制造时就已经被安装到重现装置中的值，并根据需要由 Km 更新单元 1505 更新。

EMM 加密单元 1507 用主密钥加密 EMM，并将加密的 EMM 输入到加密 EMM 发送单元 1508。

加密 EMM 发送单元 1508 向广播装置发送加密的 EMM。

用于发送其中有种子信息的 EMM 用更新之前的老的主密钥加密。更新后的新的主密钥将在加密 EMM 的下一个时机开始被使用。

如至此所解释的那样，密钥管理装置(i)生成种子信息并将其插入 EMM 中，(ii)通过广播装置向重现装置发送种子信息，(iii)利用种子信息更新主密钥 Km。另一方面，重现装置利用已经发送的种子信息更新主密钥。这里，由于密钥管理装置和重现装置各自拥有相同算法以便根据种子信息生成主密钥，所以密钥管理装置和重现装置各自拥有相同的主密钥。

图 16 表示密钥管理装置管理 ID 和主密钥的例子。

密钥管理装置用图 16 中所示的管理表管理集中在 ID/Km 存储单元的所有 ID 和主密钥。在管理表中，不同的 ID 在行的方向上排列，主密钥 Km 的不同的生成在列的方向上排列。

当密钥管理装置向制造机器分配 ID 和主密钥时，这些 ID 和主密钥被添加到这个管理表中。一开始，将一个主密钥添加到第一生成的列中，主密钥每次被更新时，新的主密钥被添加到下一列，从第二生成的列开始，然后添加到第三生成的列。

要把包括过去的主密钥在内的所有主密钥存储起来的理由，可作以下解释:

当把一个相同的 ID 分配给相同型号的每个重现装置时，未必所有

重现装置都能在第一次传送更新信息后成功地更新它们的主密钥。因此有必要向那些尚未成功地更新它们的主密钥的重现装置发送已经利用过去的主密钥进行加密的更新信息。

密钥管理装置的操作

图 17 表示条件访问装置中的密钥管理装置的操作。

当从广播装置接收 EMM 时，密钥管理装置从 EMM 中包含的标识符判断是否要需要更新密钥(S1701)。

如果主密钥需要被更新(S1702,Y)，则密钥管理装置生成种子信息(S1703)，并把种子信息插入 EMM 中(S1704)。

密钥管理装置获得存储在 ID/Km 存储单元中的主密钥(S1705)，用主密钥加密 EMM（S1706）。

然后，密钥管理装置向广播装置发送加密的 EMM(S1707)。

在步骤 S1707 向广播装置发送加密的 EMM 之后，密钥管理装置用在步骤 S1703 中生成的种子信息生成新的主密钥(S1708)。

密钥管理装置存储在步骤 S1708 中生成的新的主密钥，并从下一个时机开始使用新的主密钥(S1709)。

如果在步骤 S1702 中主密钥不需要被更新(S1702,N)，密钥管理装置获得存储在 ID/Km 存储单元中的主密钥(S1710)，用主密钥加密 EMM（S1711）。

然后，密钥管理装置向广播装置发送加密的 EMM(S1712)。

条件访问系统的操作

以下说明包括上述重现装置和密钥管理装置的条件访问系统的操作。该实施例的特征在于这样的操作，即，如果已经知道了有一个伪装成授权的重现装置的未授权的重现装置，就有可能防止未授权的重现装置观看内容。以下解释该特定操作。

图 18 表示在防止非授权装置进行非授权的内容观看时重现装置的操作。

重现装置 1 由被授权观看内容的用户 1 所有，存储着 ID1 和主密钥 Km1。同样，重现装置 2 由被授权观看内容的用户 2 所有，存储着 ID2 和主密钥 Km2。未授权重现装置伪装成重现装置 2，存储着 ID2 和主密钥 Km2。

以下解释广播装置发现有未授权的重现装置以及防止未授权的重

现装置观看内容的过程。

广播装置发送 EMM1 至重现装置 1(S1801)。

一般来说,EMM 包括(i)要接收该特定 EMM 集的重现装置的 ID,(ii)加密的工作密钥 E(Kw,Km),这是用主密钥加密了的工作密钥 Kw。相应地, EMM1 包括 ID1 和加密的工作密钥 E(Kw,Km1)。

重现装置 1 根据 EMM1 中包含的 ID1 判断该特定的 EMM 集是要发送到该重现装置 1 自己的, 就用在该重现装置 1 自身中存储的 Km1 解密 E(Kw,Km1)。结果,重现装置 1 获得工作密钥 Kw(S1802)。

广播装置发送 EMM2 至重现装置 2(S1803)。

EMM2 包括 ID2 和加密的种子信息 E(种子,Km2),加密的种子信息 E(种子,Km2)是用主密钥 Km2 加密了的种子信息 “Seed” ("种子")。

重现装置 2 根据 EMM2 中包含的 ID2 判断该特定的 EMM 集是要发送到该重现装置 2 自己的, 就用在该重现装置 2 自身中存储的 Km2 解密 E(种子,Km2)。结果,重现装置 2 获得种子信息"种子"(S1804)。

未授权的重现装置也根据 EMM2 中包含的 ID2 判断该特定的 EMM 集是要发送到该未授权的重现装置自己的, 就用在该未授权的重现装置自身中存储的 Km2 解密 E(种子,Km2)。结果,该未授权的重现装置获得种子信息"种子"(S1805)。

重现装置 2 根据种子信息"种子"生成新的主密钥 Km′2(S1806)。用来根据种子信息"种子"生成主密钥 Km′2 的算法对每个重现装置、每个生产批次、每个型号或制造商来说都是独有的。由于存储相同的算法, 密钥管理装置也能根据种子信息"种子"生成主密钥 Km′2。因此, 重现装置 2 和密钥管理装置各自都拥有相同的新的主密钥 Km′2。

另一方面, 未授权的重现装置没有用来根据种子信息"种子"生成主密钥 Km′2 的算法, 因此不能生成主密钥 Km′2(S1807)。

广播装置向重现装置 2 发送 EMM2′(S1808)。

这里, EMM2′包括 ID2 和加密的工作密钥 E(Kw,Km2′)。

重现装置 2 根据 EMM2 中包含的 ID2 判断该特定的 EMM 集是要发送到该重现装置 2 自己的, 就用在该重现装置 1 自身中存储的 Km2′解密 E(Kw,Km2′)。结果,重现装置 2 获得工作密钥 Kw(S1809)。

另一方面, 未授权的重现装置也根据 EMM2 中包含的 ID2 判断该特定的 EMM 集是要发送到该未授权的重现装置自己的, 但是不能获得工

作密钥 Kw，因为未授权重现装置没有存储主密钥 Km2′(S1810)。

广播装置向重现装置 1 和重现装置 2 都发送 ECM(S1811)。

EMM 包括加密的加扰密钥 E(Ks,Kw),这是用工作密钥 Kw 加密了的加扰密钥 Ks。

重现装置 1 接收 ECM，用在步骤 S1802 中获得的工作密钥 Kw 解密 E(Ks,Kw)。结果，重现装置 1 获得加扰密钥 Ks(S1812)。

重现装置 2 接收 ECM，并用在步骤 S1809 中获得的工作密钥解密 E(Ks,Kw)。结果，重现装置 2 获得加扰密钥 Ks(S1813)。

另一方面，未授权重现装置在步骤 S1810 不能获得工作密钥 Kw，因此也不能获得加扰密钥 Ks(S1814)。

广播装置向重现装置 1 和重现装置 2 中的每一个发送加扰内容(S1815)。

加扰的内容 E(内容,Ks)是被用加扰密钥 Ks 加扰了的内容。

重现装置 1 用在步骤 S1812 中获得的加扰密钥 Ks 解扰内容 E(内容,Ks)。结果，重现装置 1 获得内容(S1816)。

重现装置 2 用在步骤 S1813 中获得的加扰密钥 Ks 解扰内容 E(内容,Ks)。结果，重现装置 2 获得内容(S1817)。

另一方面，未授权的重现装置在步骤 S1814 不能获得加扰密钥 Ks，因此也不能获得内容(S1818)。

这样，当获知有未授权的重现装置伪装成授权的重现装置时，广播装置更新由密钥管理装置和重现装置二者都拥有的主密钥，并因此能防止未授权的重现装置观看内容。

在这个实施例中，由于主密钥是运用广播发送的 EMM 更新的，更新主密钥要比用诸如 IC 卡等便携式介质来传送时快几天。因此，授权用户将不会受到在便携式介质到达之前可能导致的不能享有观看所需内容的特权的损失。

此外，密钥管理装置无需承担向所有需要便携式介质的重现装置发送便携式介质的成本，即使是向每个生产批次、每个型号或每个制造商而不是向每个重现装置分配一个 ID 和主密钥也是如此。

第二实施例

条件访问系统的总体结构

图 19 表示第二实施例的条件访问系统的总体结构。

第二实施例的条件访问系统包含密钥管理装置 1901、制造机器 1902、重现装置 1903 和广播装置 1904。

密钥管理装置 1901 和重现装置 1903 各自拥有相同的 ID 和相同的主密钥 Km 的程序以及重现装置 1903 获得工作密钥 Kw 的程序与第一实施例中的相同。

第二实施例与第一实施例的区别在于更新主密钥 Km 的方法。

在第二实施例中，主密钥按以下方式更新:

广播装置 1904 在 EMM 中存储(i)需要对主密钥更新的重现装置的 ID 和(ii)指示主密钥需要被更新的触发信息，并广播 EMM。然后，需要更新的主密钥的重现装置由于更新信息而认为主密钥 Km 需要得到更新，就向密钥管理装置 1901 发送诸如其自己的 ID 的装置信息。密钥管理装置 1901 向重现装置发送要由其生成新的主密钥的种子信息。重现装置用种子信息更新主密钥 Km。

这里，由于只有密钥管理装置和授权的用户的重现装置存储用来根据种子信息生成主密钥 Km′s 的相同算法，因此只有密钥管理装置和授权用户的重现装置能够有相同的新的主密钥 Km′s。因此，条件访问系统就能在主密钥被更新后防止未授权的重现装置非法观看内容。

在第一实施例中，将种子信息存储在 EMM 中，然后传送 EMM。第二实施例与第一实施例的区别在于所传送的 EMM 存储着触发信息，该信息只是启动对主密钥的更新，而种子信息则不在 EMM 中而是以其它方式传送。

以下详细解释实现这种条件访问系统的重现装置。

重现装置的结构

第二实施例的重现装置与第一实施例的重现装置的区别仅在于 Km 更新单元。因此将仅解释 Km 更新单元，而省略对该结构的其它部分的解释。

图 20 表示第二实施例中 Km 更新单元的详细结构。

Km 更新单元包含装置信息存储单元 2001，装置信息发送单元 2002，种子信息接收单元 2003，Km 生成单元 2004，和 Km 保留单元 2005。

装置信息存储单元 2001 存储重现装置独有的装置信息，诸如 ID，并按照来自更新信息判断单元的通知而向装置信息发送单元 2002 输入

装置信息。

装置信息发送单元 2002 把装置信息存储单元 2001 中存储的装置信息发送到密钥管理装置，以作为请求种子信息的请求信号。响应对装置信息的接收，密钥管理装置相应地发送回种子信息。

种子信息接收单元 2003 接收种子信息并把种子信息输入到 Km 生成单元 2004，以作为用于生成主密钥的算法中的参数。这里，装置信息和种子信息是通过电话线传输的。

Km 生成单元 2004 用已经安装在 Km 生成单元自身中的算法生成一个新的主密钥 Km′。该算法对每个重现装置、每个生产批次、每个型号或每个制造商来说是独特的。相同的算法也存储在密钥管理装置中。

Km 保留单元 2005 保留主密钥。

在该实施例中，根据新的主密钥的生成的时刻，也有下文所述的两种可能，可以是任何一种可能。

第一种可能是，一旦获得种子信息就生成新的主密钥。

第二种可能是，种子信息获得后被存储起来，直到需要生成新的主密钥。在这种情况下，例如可以在 EMM 被输入到 EMM 解密单元后，然后收到从 EMM 解密单元发送的信号之后，生成新的主密钥。

图 21 表示用于更新主密钥 Km 的 EMM 的数据结构。

在这个实施例中，将标识符存储在数据段中，该标识符本身就是触发信息。

密钥管理装置的结构

图 22 表示条件访问系统中的密钥管理装置的结构。

密钥管理装置 2201 包含 EMM 接收单元 2202、密钥更新判断单元 2203、种子信息生成单元 2204、Km 更新单元 2205、ID/Km 存储单元 2206、EMM 加密单元 2207、加密 EMM 发送单元 2208、装置信息接收单元 2209 和种子信息发送单元 2210。

第二实施例中的密钥管理装置与第一实施例中的不同之处在于种子信息生成单元 2204、装置信息接收单元 2209 和种子信息发送单元 2210。因此，只解释结构的这些相同的部分，而省略对相同结构的解释。

种子信息生成单元 2204 从密钥更新判断单元 2203 接收通知，生成种子信息，将种子信息输入到 Km 更新单元 2205 以及种子信息发送

单元 2210。种子信息是要由其生成新的主密钥的信息，例如可以是主密钥 Km 的生成数或者随机数。

装置信息接收单元 2209 从重现装置接收诸如 ID 的装置信息，并识别已经发送该装置信息的特定重现装置。

种子信息发送单元 2210 向装置信息接收单元 2209 所标识的重现装置发送种子信息。

这样，在本实施例中，密钥管理装置按照重现装置对种子信息的请求而发送种子信息。重现装置由于 EMM 中包含的触发信息而意识到主密钥需要被更新，于是向密钥管理装置发送对种子信息的请求。

于是，重现装置和密钥管理装置各自含有相同的种子信息，它们各自将运用相同的算法根据种子信息而生成新的主密钥。

在本实施例中，重现装置在更新主密钥时需要与密钥管理装置通信；因此，密钥管理装置能够识别由其衍生了未授权的重现装置的那个重现装置。

例如，如果安排得使得各个重现装置需要发送它们自己的 ID 作为请求信号并且存在着一个未授权的重现装置，则同一个 ID 将被多于一次地发送到密钥管理装置。这样，密钥管理装置就能判断出具有该特定 ID 的重现装置就是由其衍生了该未授权的重现装置的那个重现装置。

应当注意的是，本实施例中，装置信息和种子信息是通过电话线传送的；然而，传送方式并非仅限于此，也可以离线(off line)传送。种子信息也可以用 EMM 传送。

第三实施例

图 23 表示第三实施例的条件访问系统的总体结构。

第三实施例的条件访问系统包含密钥管理装置 2301、制造机器 2302、重现装置 2303 和广播装置 2304。

密钥管理装置 2301 和重现装置 2303 各自拥有相同的 ID 和相同的主密钥 Km 的程序以及重现装置 2303 获得工作密钥 Kw 的程序与第一实施例中的相同。

第三实施例与第一实施例的区别在于更新主密钥 Km 的方法。

在第三实施例中，主密钥按以下方式更新：

广播装置 2304 在 EMM 中存储(i)需要对主密钥更新的重现装置 2303

的 ID 和(ii)要由其生成新的主密钥 Km′的种子信息，并广播 EMM。

重现装置 2303 由于种子信息而意识到主密钥 Km 需要得到更新，就生成事件信息，并根据种子信息和事件信息二者生成新的主密钥 Km′。这里，事件信息表示对每个更新有不同的值的信息。在本实施例中，随机数被用作事件信息。

重现装置 2303 然后向密钥管理装置 2301 发送包括重现装置 2303 自己的 ID 的装置信息和随机数。密钥管理装置 2301 用种子信息和随机号码二者更新主密钥。

这里，由于只有密钥管理装置和授权用户的重现装置存储相同的用来根据种子信息和随机号码生成新的主密钥 Km′的算法，所以只有密钥管理装置和授权用户的重现装置才能有相同的新的主密钥 Km′s。

因此，条件访问系统就能在主密钥被更新后防止未授权的重现装置观看内容。

以下详细解释实现这种条件访问系统的重现装置。

重现装置的结构

第三实施例的重现装置与第一实施例的重现装置的区别仅在于 Km 更新单元。因此将仅解释 Km 更新单元，而省略对该结构的其它部分的解释。

图 24 表示第三实施例中 Km 更新单元的详细结构。

Km 更新单元包含种子信息获得单元 2401、装置信息生成单元 2402,Km 生成单元 2403、Km 保留单元 2404 和装置信息发送单元 2405。

种子信息获得单元 2401 从更新信息判断单元获得种子信息并把种子信息输入到 Km 生成单元 2403，作为用于生成主密钥的算法中的参数。

装置信息生成单元 2402 响应来自更新信息判断单元的通知而生成随机数，将随机数与已经存储在装置信息生成单元 2402 本身中的 ID 组合，生成重现装置独有的装置信息。装置信息被输入到 Km 生成单元 2403 和装置信息发送单元 2405 中。

Km 生成单元 2303 用已经安装在 Km 生成单元 2303 自身中的算法生成一个新的主密钥 Km′。该算法对每个重现装置、每个生产批次、每个型号或每个制造商来说是独特的。相同的算法也存储在密钥管理装置中。

Km保留单元2404保留主密钥Km。

装置信息发送单元2305把装置信息生成单元2302所生成的装置信息发送到密钥管理装置。这里，装置信息和种子信息是通过电话线传输的。

在该实施例中，根据新的主密钥的生成的时刻，也有下文所述的两种可能，可以是任何一种可能。

第一种可能是，一旦获得种子信息就生成新的主密钥。

第二种可能是，种子信息获得后被存储起来，直到需要生成新的主密钥。在这种情况下，例如可以在EMM被输入到EMM解密单元后，然后收到从EMM解密单元发送的信号之后，生成新的主密钥。

密钥管理装置的结构

图25表示条件访问系统中的密钥管理装置的结构。

第三实施例中的密钥管理装置与第一实施例中的不同之处在于装置信息接收单元2505和Km更新单元2506。因此，只解释装置信息接收单元，而省略对结构的其它部件的解释。

装置信息接收单元2505从重现装置接收装置信息。装置信息由重现装置的ID和在重现装置中生成的随机数组成。装置信息接收单元2505用其中包含的ID来标识已经发送这个装置信息的特定重现装置。

Km更新单元2506用种子信息生成和插入单元2504所生成的种子信息和装置信息接收单元2505所接收的随机数二者来更新主密钥。

新的主密钥是运用与在重现装置中存储的算法相同的算法生成的。

这样，在本实施例中，密钥管理装置在EMM中存储中子信息且向重现装置发送EMM，并从重现装置接收随机数。重现装置由于种子信息而意识到主密钥需要被更新，于是向密钥管理装置发送生成的随机数。

于是，重现装置和密钥管理装置各自获得相同的种子信息和相同的随机数，各自运用相同的算法根据种子信息和随机数而生成新的主密钥。

在本实施例中，重现装置在更新主密钥时需要与密钥管理装置通信；因此，密钥管理装置能够识别由其衍生了未授权的重现装置的那

个重现装置。

例如，如果安排得使得重现装置需要发送它们自己的 ID 作为请求信号并且有一个未授权的重现装置，则同一个 ID 将被多于一次地发送到密钥管理装置。这样，密钥管理装置就能判断出具有该特定 ID 的重现装置就是由其衍生了未授权重现装置的那个重现装置。

应当注意的是，本实施例中，装置信息和种子信息是通过电话线传送的；然而，传送方式并非仅限于此，它们也可以离线传送。

在上述的所有实施例中，重现装置和密钥管理装置只更新主密钥；然而，不仅更新主密钥，也更新 ID，这也是可以接受的。主密钥和 ID 可以通过被覆写而被更新，也可以这样安排，即将一些 ID 存储起来，这些存储的 ID 是有效的，或者将所有 ID 存储起来，所有这些 ID 是有效的。

在上述的所有实施例中，用来生成新的主密钥的算法是由密钥管理装置管理的，然而，只要具备安全的状态，本发明就不局限于此。例如，如果有多个制造商，每个制造商管理用于其自己的重现装置的算法，则有分散风险的有益效果，因为对多个算法是分别管理的。

在第一实施例中，更新主密钥的方法仅应用于条件访问系统中的重现装置；然而，也可能将该更新主密钥的方法应用于其它的、为了保护各种信息而具有对应于 ID 的密钥的装置，例如 SD 卡和 DVD 重现装置。以下解释将该更新方法应用于 DVD 重现装置的例子。

图 26 表示 DVD 重现装置的结构。

重现装置 2601 包含读取单元 2602、类型判断单元 2603、设备密钥存储单元 2604、媒体密钥解密单元 2605、更新信息判断单元 2606、内容密钥解密单元 2607、内容解扰单元 2608 和内容重现单元 2609。读取单元 2602 从 DVD 读取各种信息，类型判断单元 2603 根据信息的类型将信息传送到不同的目的地。

媒体密钥解密单元 2605 用存储在设备密钥存储单元 2604 中的设备密钥解密数据，然后将数据输入到更新信息判断单元 2606。

如果数据包括更新信息，更新信息判断单元 2606 将数据输入到设备密钥更新单元 2610；如果数据不包括更新信息，则将数据输入到内容密钥解密单元 2607。

设备密钥更新单元 2610 用更新信息生成新的设备密钥并更新在设

备密钥存储单元 2604 中存储的设备密钥。

这样，重现装置就能运用更新信息判断单元 2606 和设备密钥更新单元 2610 来更新设备密钥。

实用性

本发明适用于条件访问系统中的数字调谐器(tuner)。使用了本发明，主密钥只在授权的数字调谐器中-而不在非授权的数字调谐器中-被正确地更新。因此就有可能防止非授权的数字调谐器观看内容。此外，由于运用广播来更新主密钥，对主密钥的更新，方法容易，成本不高。

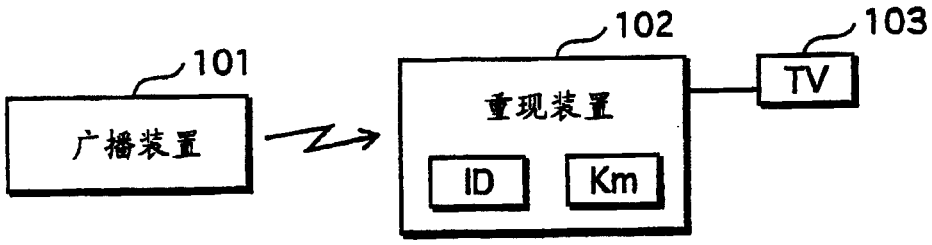


图 1 现有技术

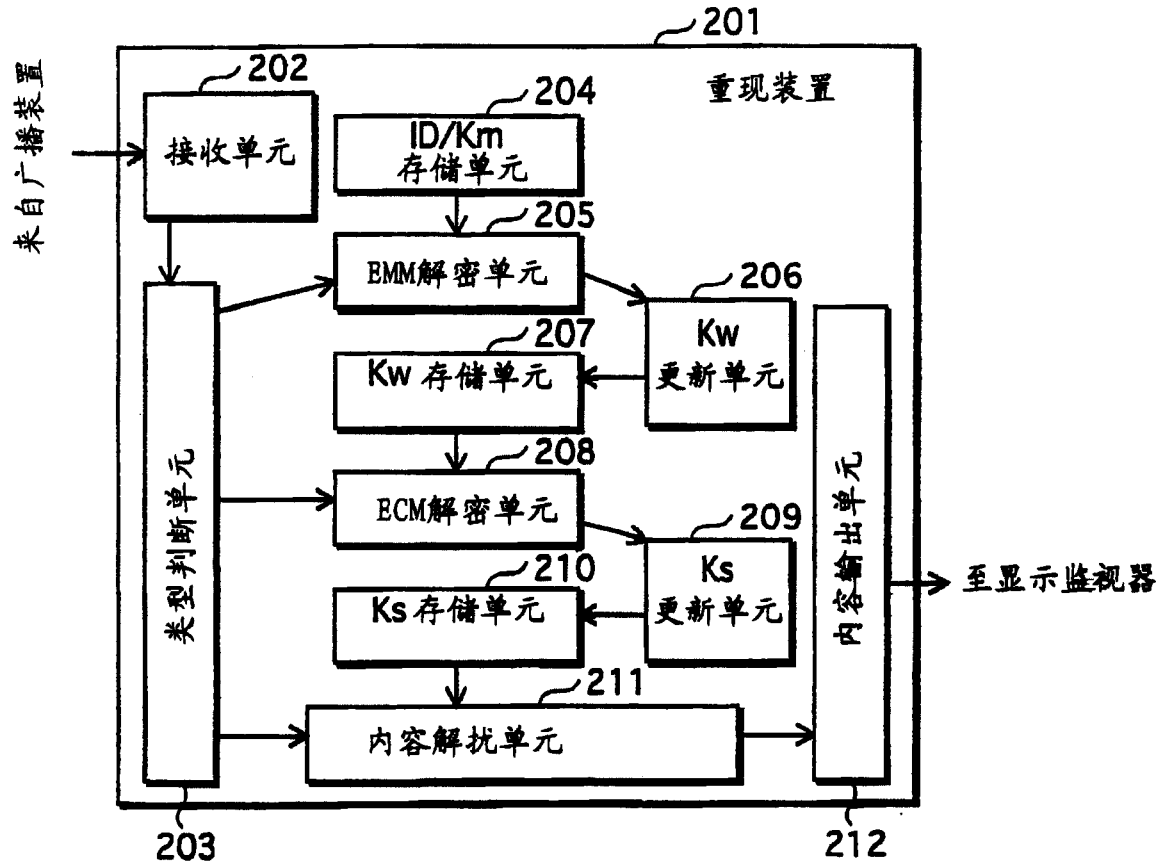

201
重现装置
202
接收单元
204
ID/Km
存储单元
205
EMM解密单元
206
Kw
更新单元
207
Kw 存储单元
208
ECM解密单元
209
Ks
更新单元
210
Ks 存储单元
211
内容解扰单元
类型判断单元
内容输出单元
来自广播装置
至显示监视器
203
212

图 2 现有技术

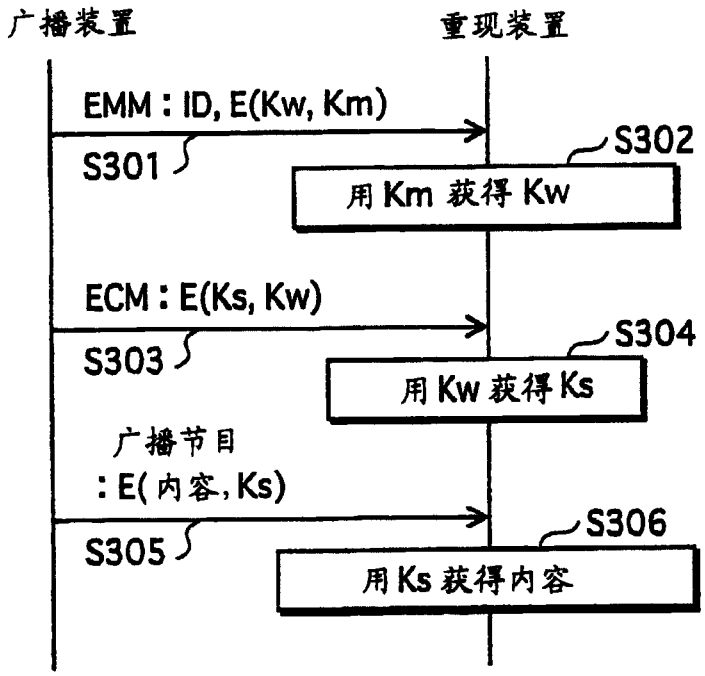

广播装置
重现装置
EMM：ID, E(Kw, Km)
S301
S302
用 Km 获得 Kw
ECM：E(Ks, Kw)
S303
S304
用 Kw 获得 Ks
广播节目
：E(内容, Ks)
S305
S306
用 Ks 获得内容

图 3 现有技术

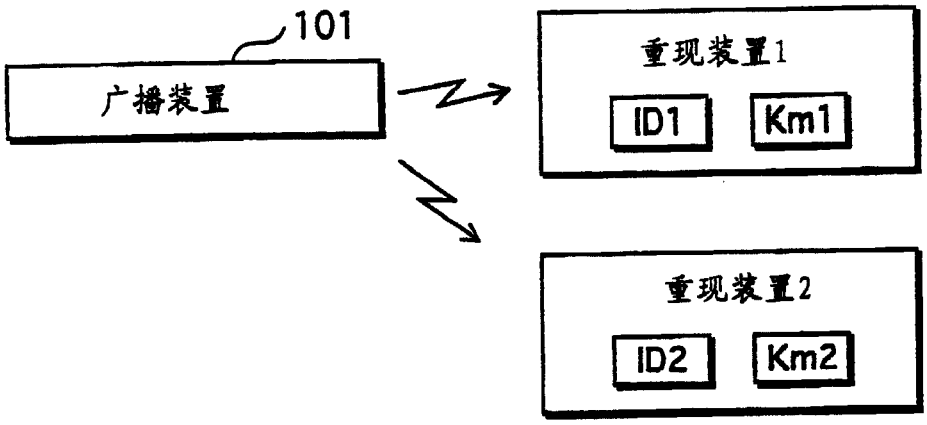


图 4 现有技术

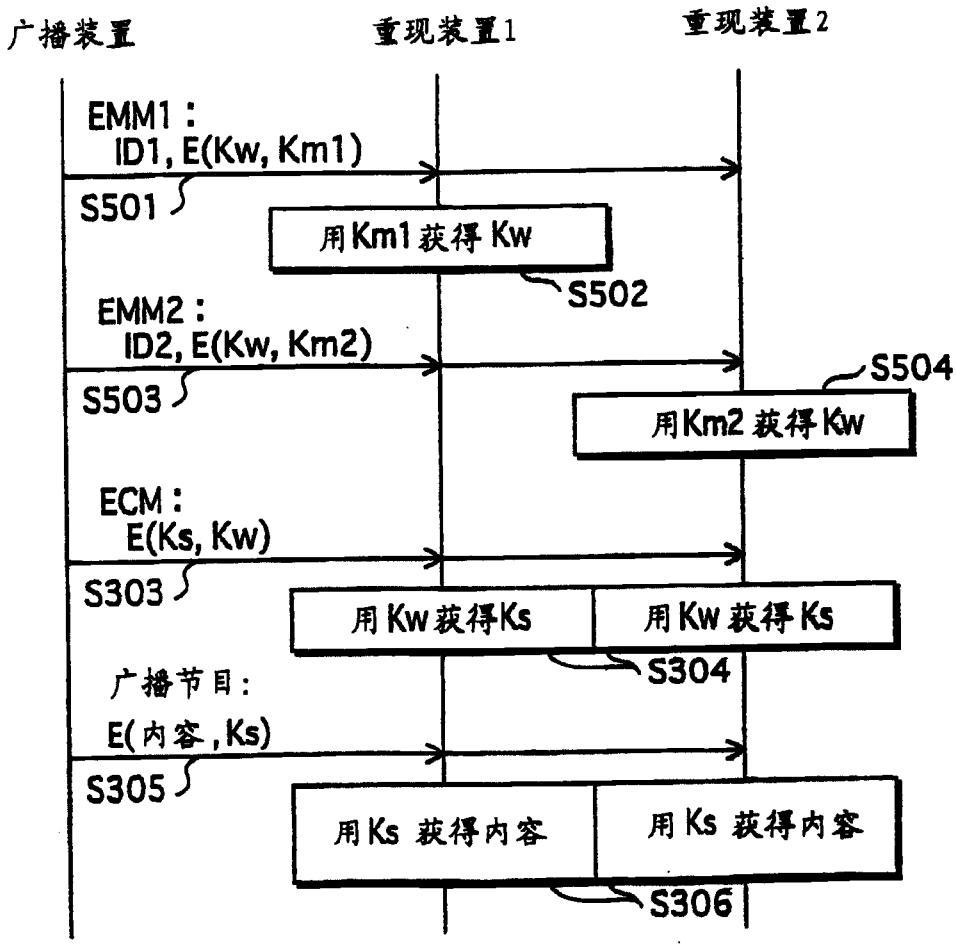

广播装置
重现装置1
重现装置2
EMM1：
ID1, E(Kw, Km1)
S501
用Km1获得Kw
S502
EMM2：
ID2, E(Kw, Km2)
S503
S504
用Km2获得Kw
ECM：
E(Ks, Kw)
S303
用Kw获得Ks
用Kw获得Ks
S304
广播节目：
E(内容, Ks)
S305
用Ks 获得内容
用Ks 获得内容
S306

图 5 现有技术

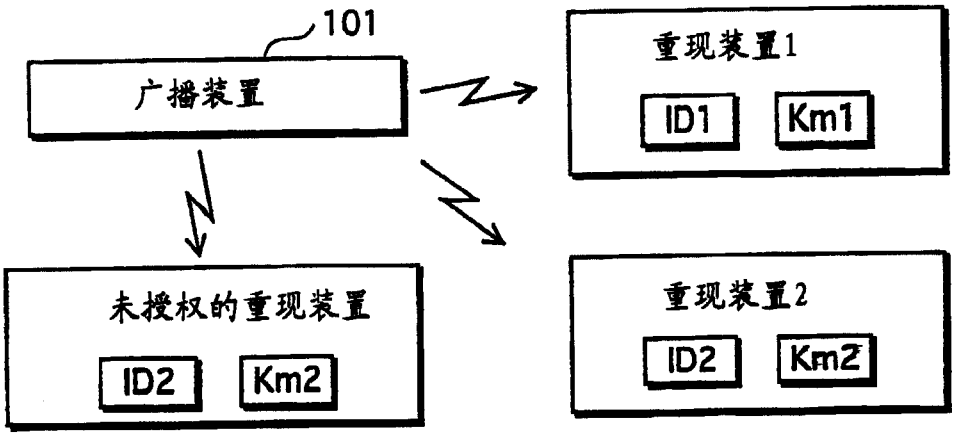


图 6 现有技术

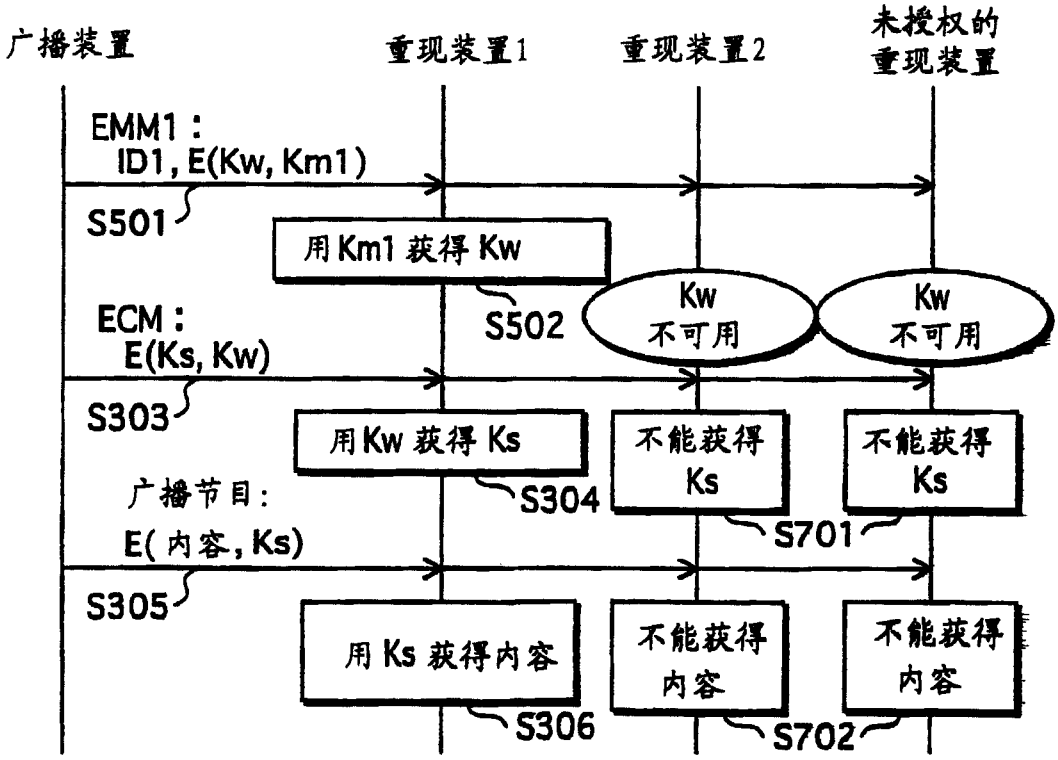

广播装置
重现装置1
重现装置2
未授权的
重现装置
EMM1：
ID1, E(Kw, Km1)
S501
用Km1 获得 Kw
S502
Kw
不可用
Kw
不可用
ECM：
E(Ks, Kw)
S303
用Kw 获得 Ks
S304
不能获得
Ks
不能获得
Ks
S701
广播节目：
E(内容, Ks)
S305
用Ks 获得内容
S306
不能获得
内容
不能获得
内容
S702

图 7现有技术

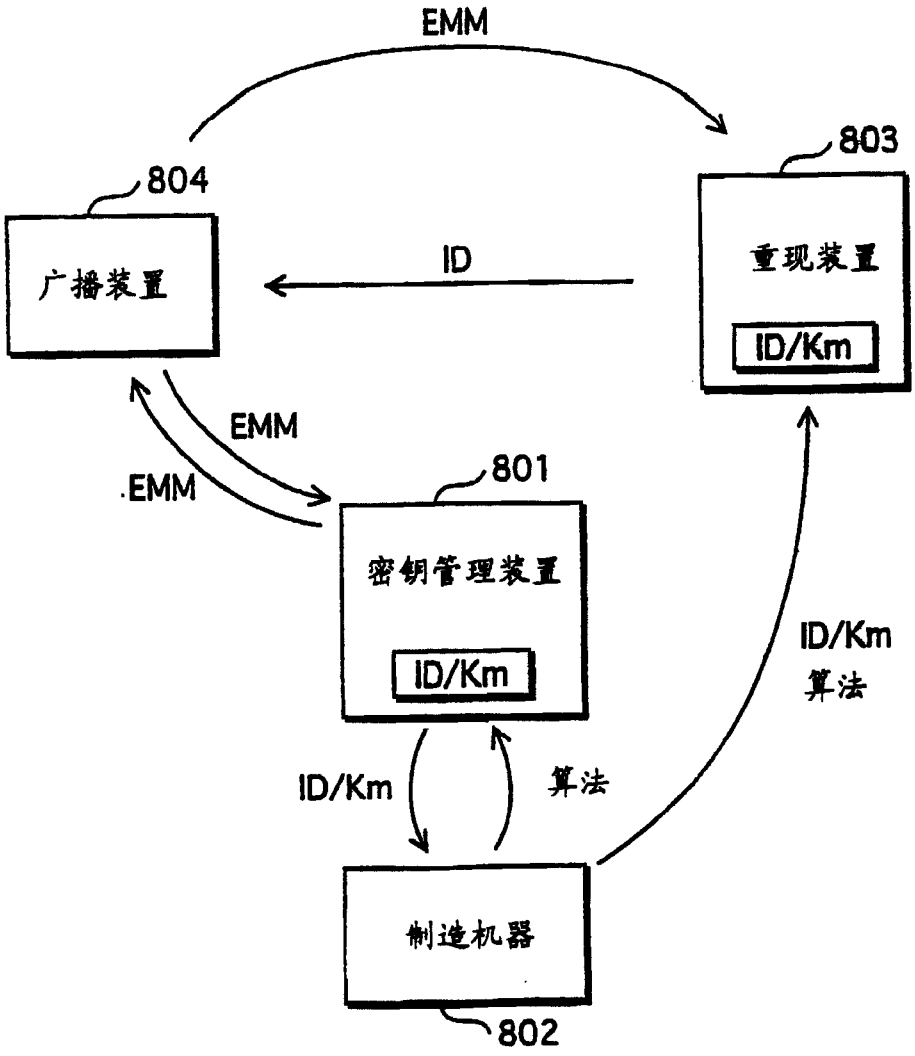

EMM
803
804
广播装置
ID
重现装置
ID/Km
EMM
EMM
801
密钥管理装置
ID/Km
ID/Km
算法
ID/Km
算法
制造机器
802

图 8

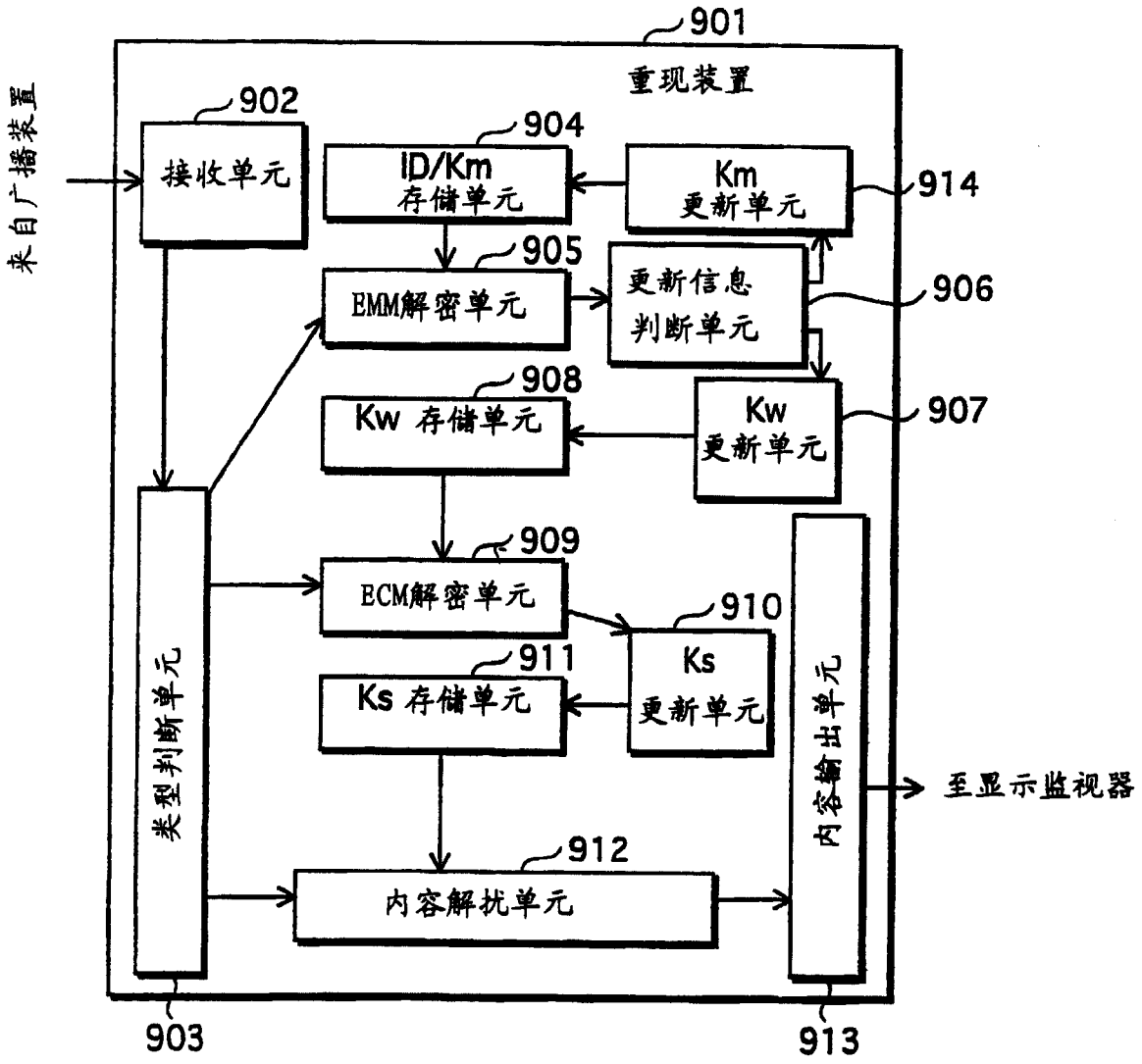

901
重现装置
来自广播装置
902
接收单元
904
ID/Km
存储单元
Km
更新单元
914
905
EMM解密单元
更新信息
判断单元
906
908
Kw 存储单元
Kw
更新单元
907
909
ECM解密单元
910
Ks
更新单元
911
Ks 存储单元
类型判断单元
912
内容解扰单元
内容输出单元
至显示监视器
903
913

图 9

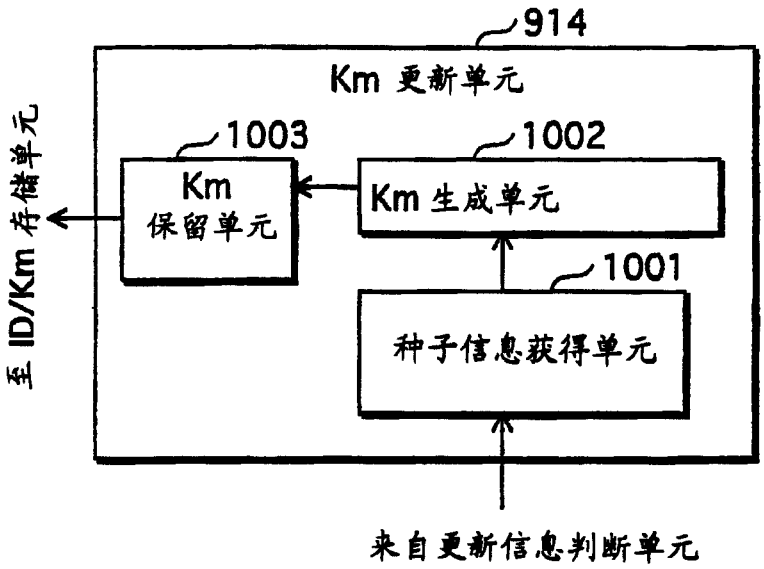

914
Km 更新单元
1003
1002
Km
保留单元
Km 生成单元
1001
种子信息获得单元
至 ID/Km 存储单元
来自更新信息判断单元

图 10

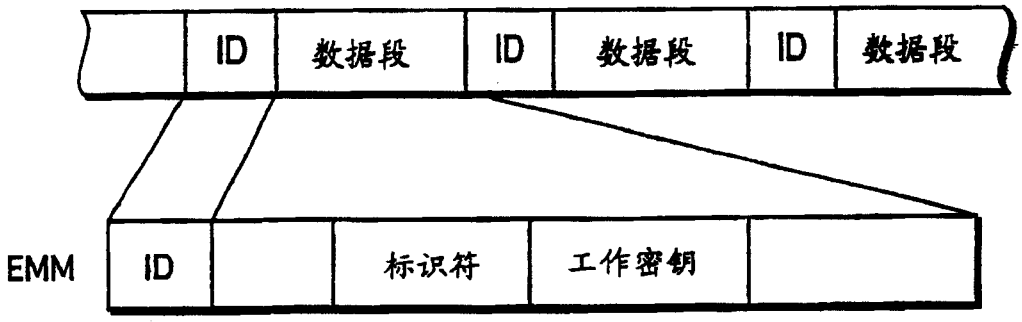


图 11

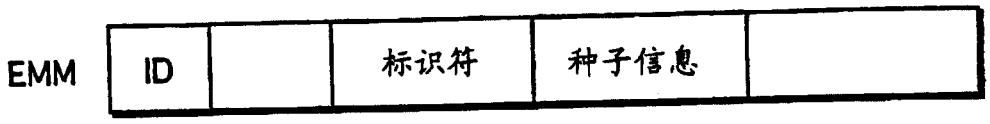


图 12

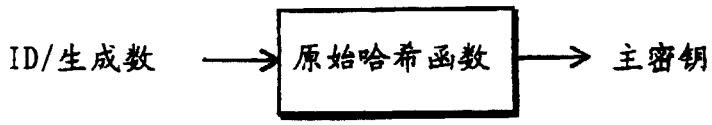


图 13A

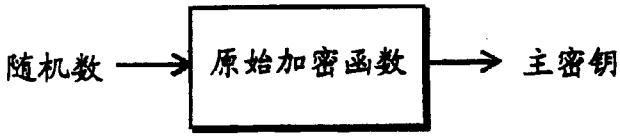


图 13B

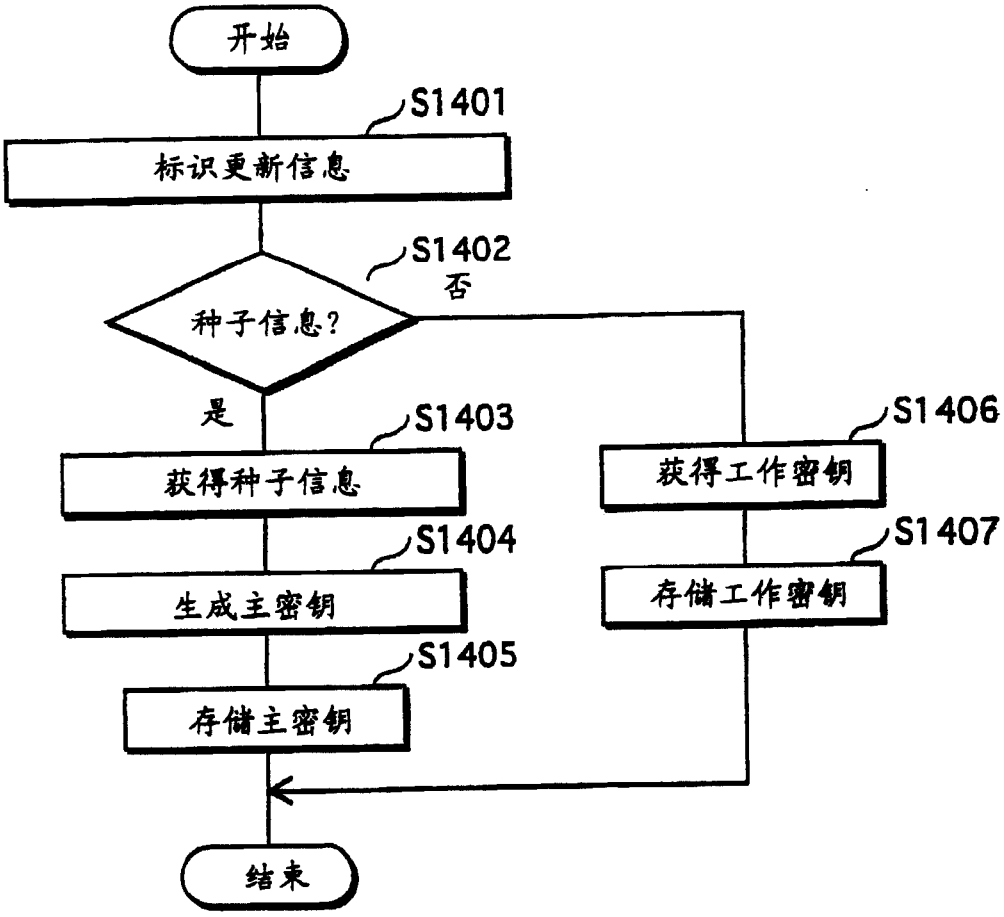

开始
S1401
标识更新信息
S1402
否
种子信息?
是
S1403
获得种子信息
S1404
生成主密钥
S1405
存储主密钥
S1406
获得工作密钥
S1407
存储工作密钥
结束

图 14

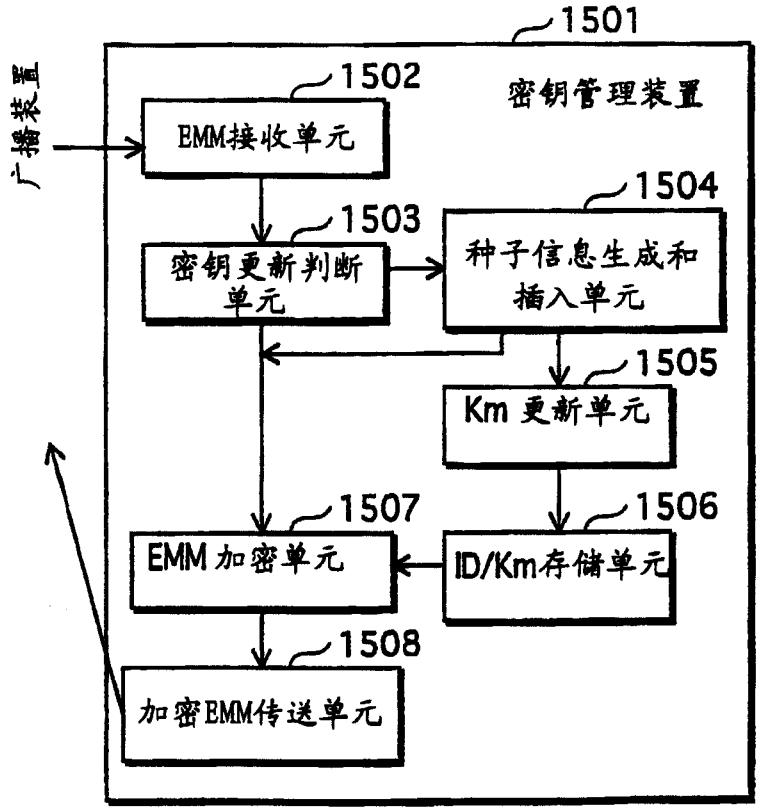

1501
密钥管理装置
1502
EMM接收单元
1503
密钥更新判断单元
1504
种子信息生成和插入单元
1505
Km 更新单元
1506
ID/Km存储单元
1507
EMM 加密单元
1508
加密EMM传送单元

图 15

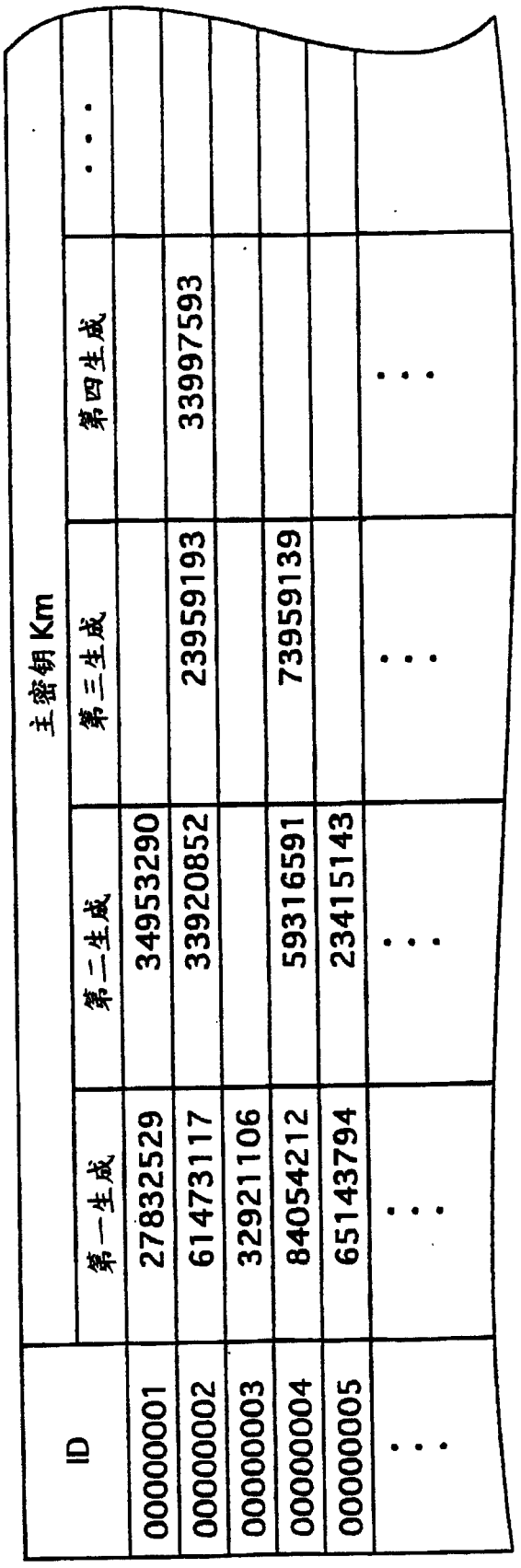

主密钥 Km
ID
第一生成
第二生成
第三生成
第四生成
00000001
27832529
34953290
00000002
61473117
33920852
23959193
33997593
00000003
32921106
00000004
84054212
59316591
73959139
00000005
65143794
23415143

图 16

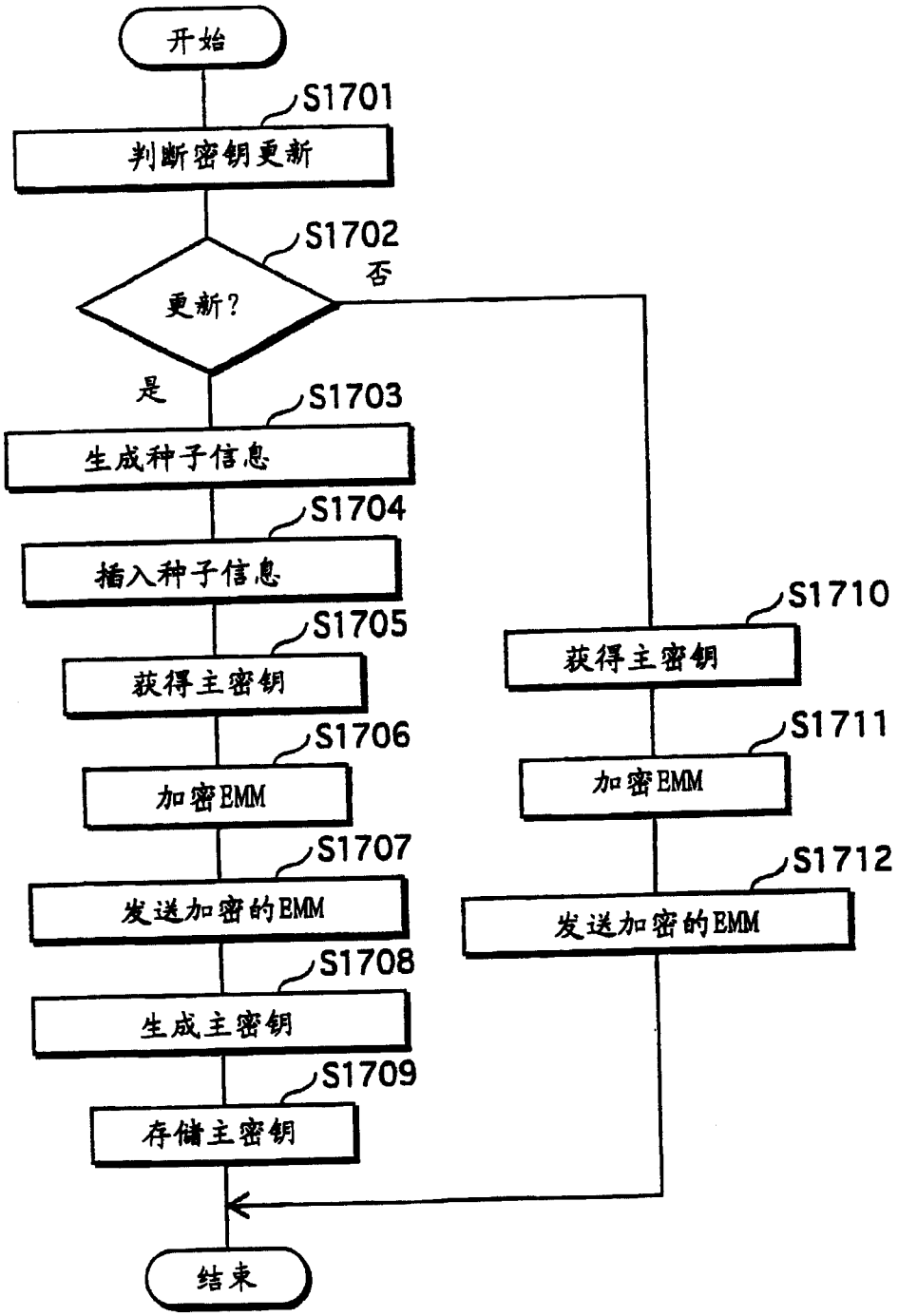

开始
S1701
判断密钥更新
S1702
更新?
否
是
S1703
生成种子信息
S1704
插入种子信息
S1705
获得主密钥
S1706
加密EMM
S1707
发送加密的EMM
S1708
生成主密钥
S1709
存储主密钥
S1710
获得主密钥
S1711
加密EMM
S1712
发送加密的EMM
结束

图 17

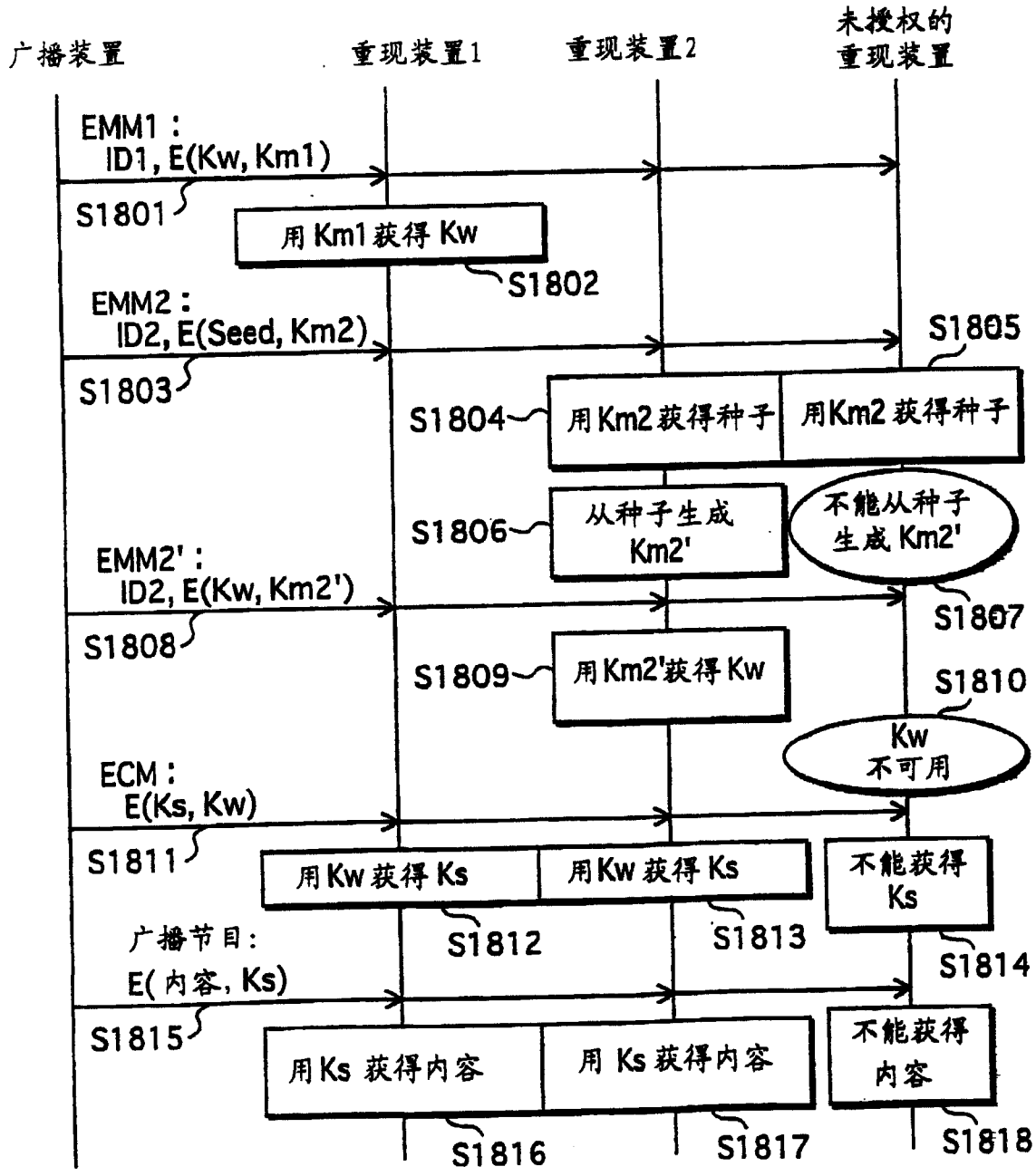

广播装置
重现装置1
重现装置2
未授权的
重现装置
EMM1：
ID1, E(Kw, Km1)
S1801
用Km1获得Kw
S1802
EMM2：
ID2, E(Seed, Km2)
S1803
S1804
用Km2获得种子
用Km2获得种子
S1805
S1806
从种子生成
Km2'
不能从种子
生成Km2'
S1807
EMM2'：
ID2, E(Kw, Km2')
S1808
S1809
用Km2'获得Kw
S1810
Kw
不可用
ECM：
E(Ks, Kw)
S1811
用Kw获得Ks
用Kw获得Ks
不能获得
Ks
S1812
S1813
S1814
广播节目：
E(内容, Ks)
S1815
用Ks获得内容
用Ks获得内容
不能获得
内容
S1816
S1817
S1818

图 18

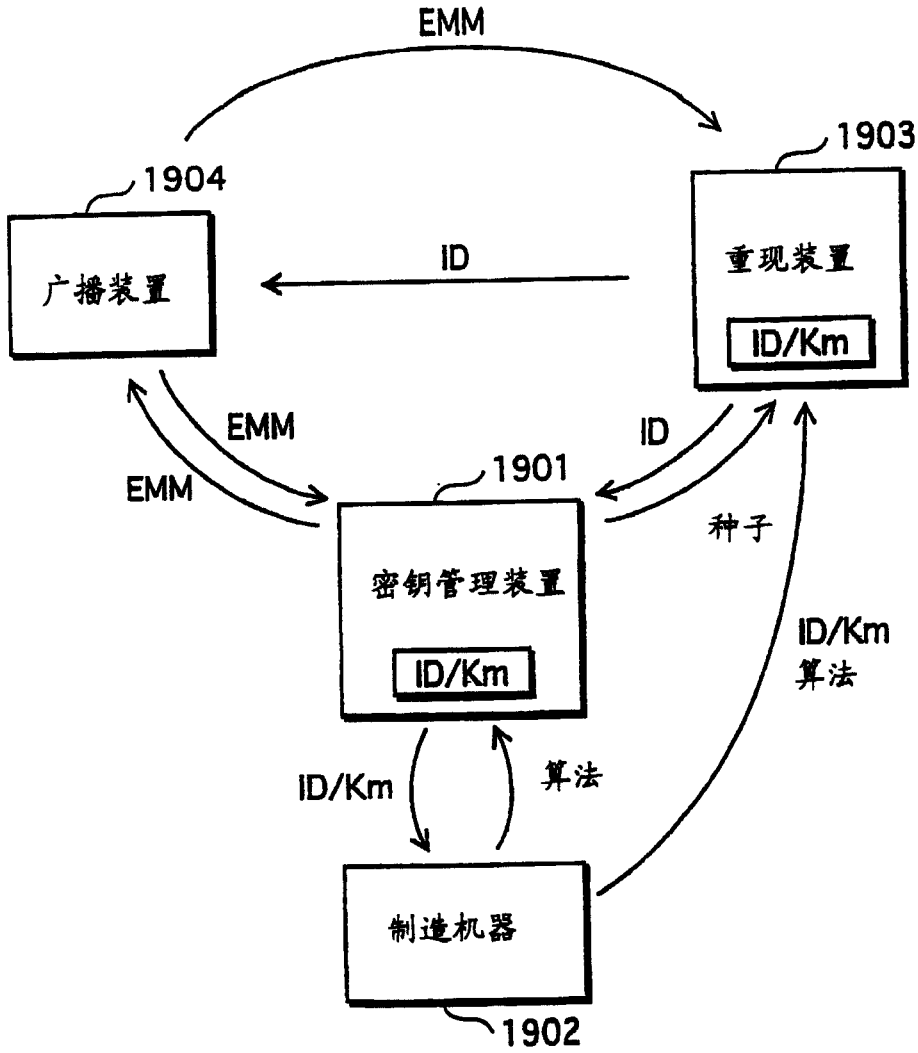

EMM
1903
1904
广播装置
ID
重现装置
ID/Km
EMM
EMM
ID
1901
种子
密钥管理装置
ID/Km
ID/Km
算法
ID/Km
算法
制造机器
1902

图 19

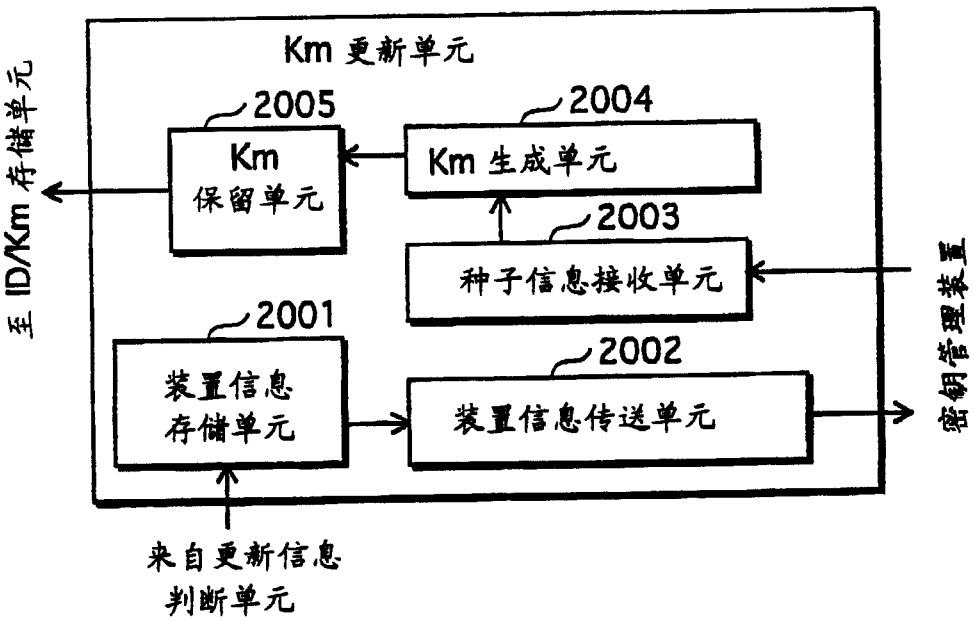

Km 更新单元
2005
Km
保留单元
2004
Km 生成单元
2003
种子信息接收单元
2001
装置信息
存储单元
2002
装置信息传送单元
至 ID/Km 存储单元
密钥管理装置
来自更新信息
判断单元

图 20

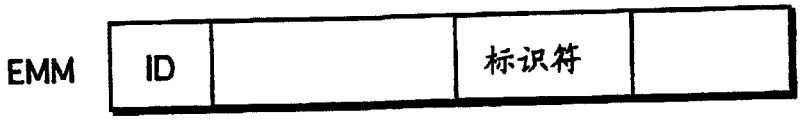


图 21

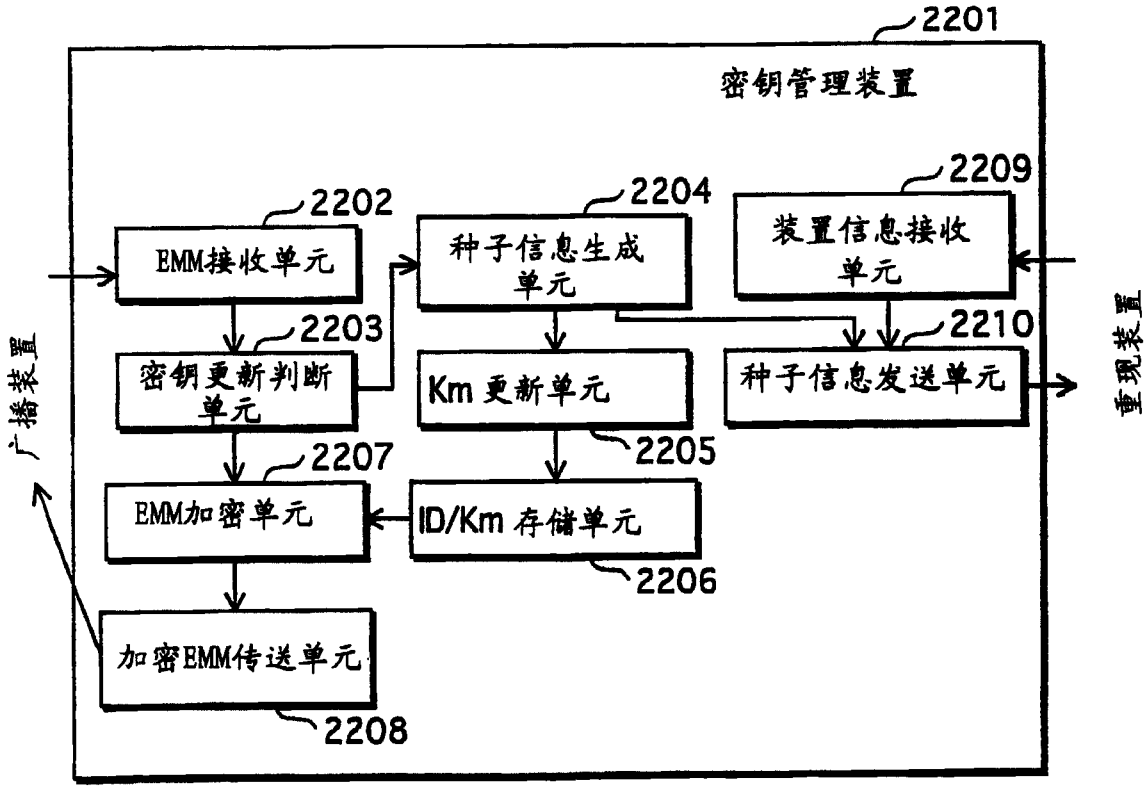

2201
密钥管理装置
2202
EMM接收单元
2204
种子信息生成单元
2209
装置信息接收单元
2203
密钥更新判断单元
Km 更新单元
2210
种子信息发送单元
2205
2207
EMM加密单元
ID/Km 存储单元
2206
加密EMM传送单元
2208
广播装置
重现装置

图 22

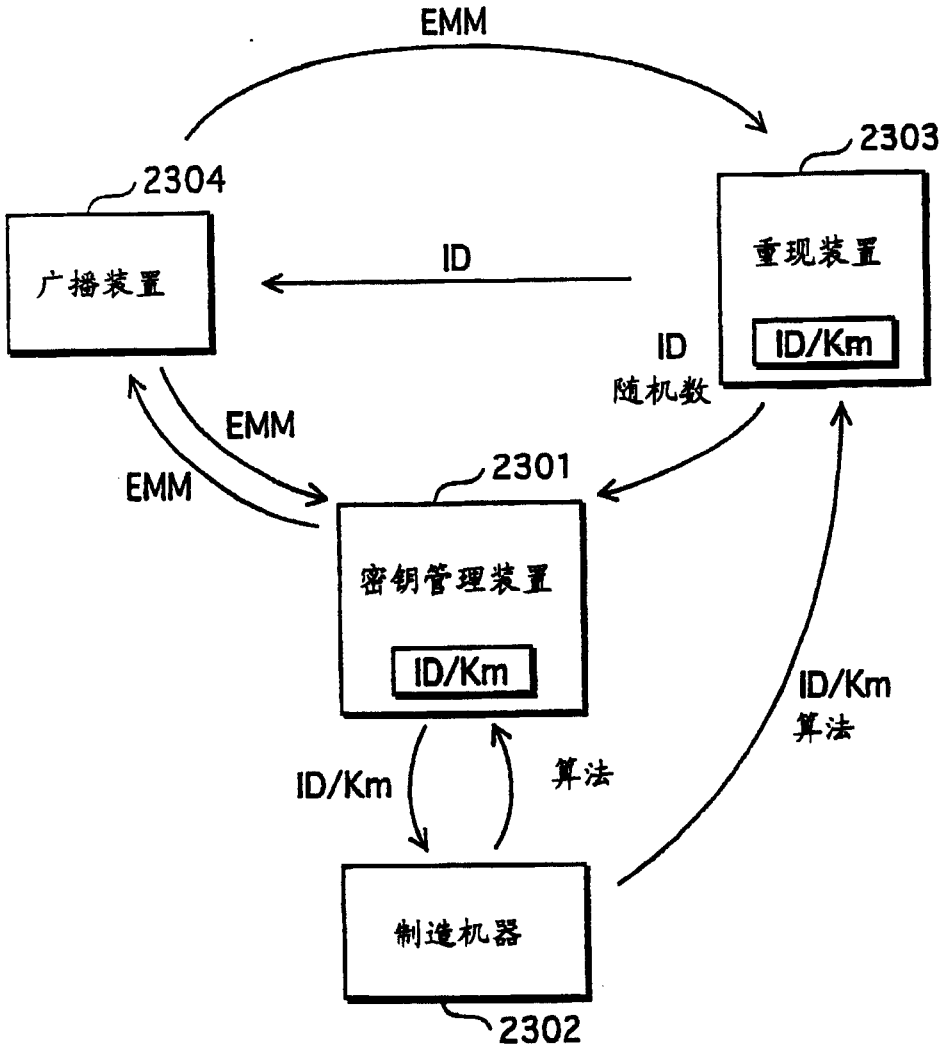

EMM
2303
2304
广播装置
ID
重现装置
ID/Km
ID
随机数
EMM
EMM
2301
密钥管理装置
ID/Km
ID/Km
算法
ID/Km
算法
制造机器
2302

图 23

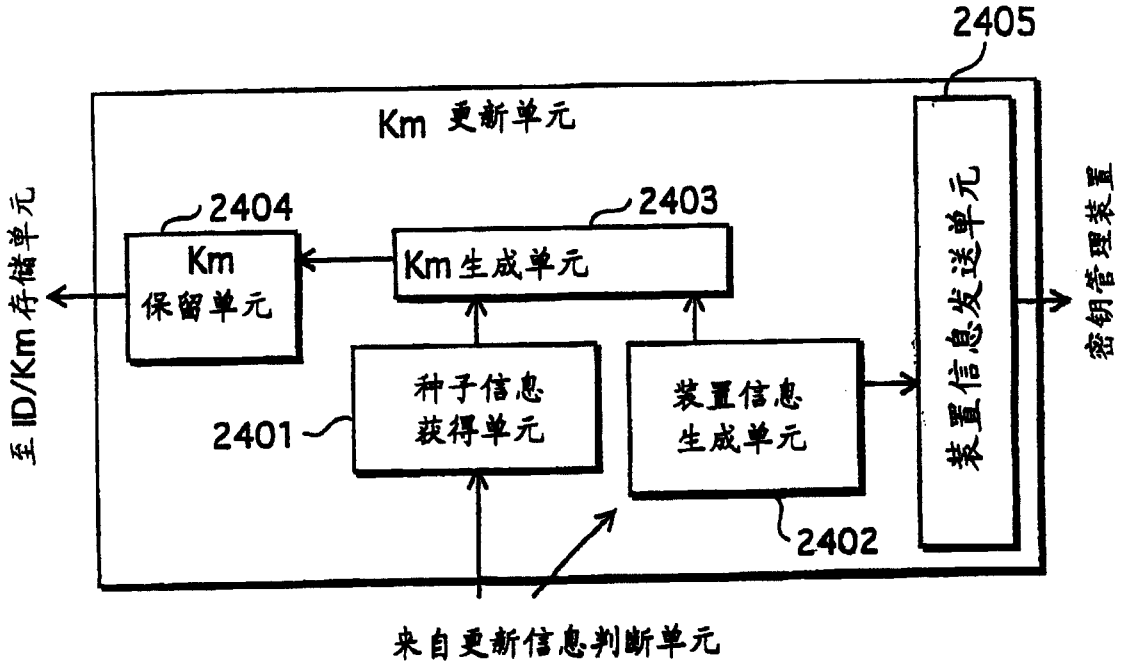

2405
Km 更新单元
2404
Km
保留单元
2403
Km生成单元
种子信息
获得单元
2401
装置信息
生成单元
2402
装置信息发送单元
至ID/Km存储单元
密钥管理装置
来自更新信息判断单元

图 24

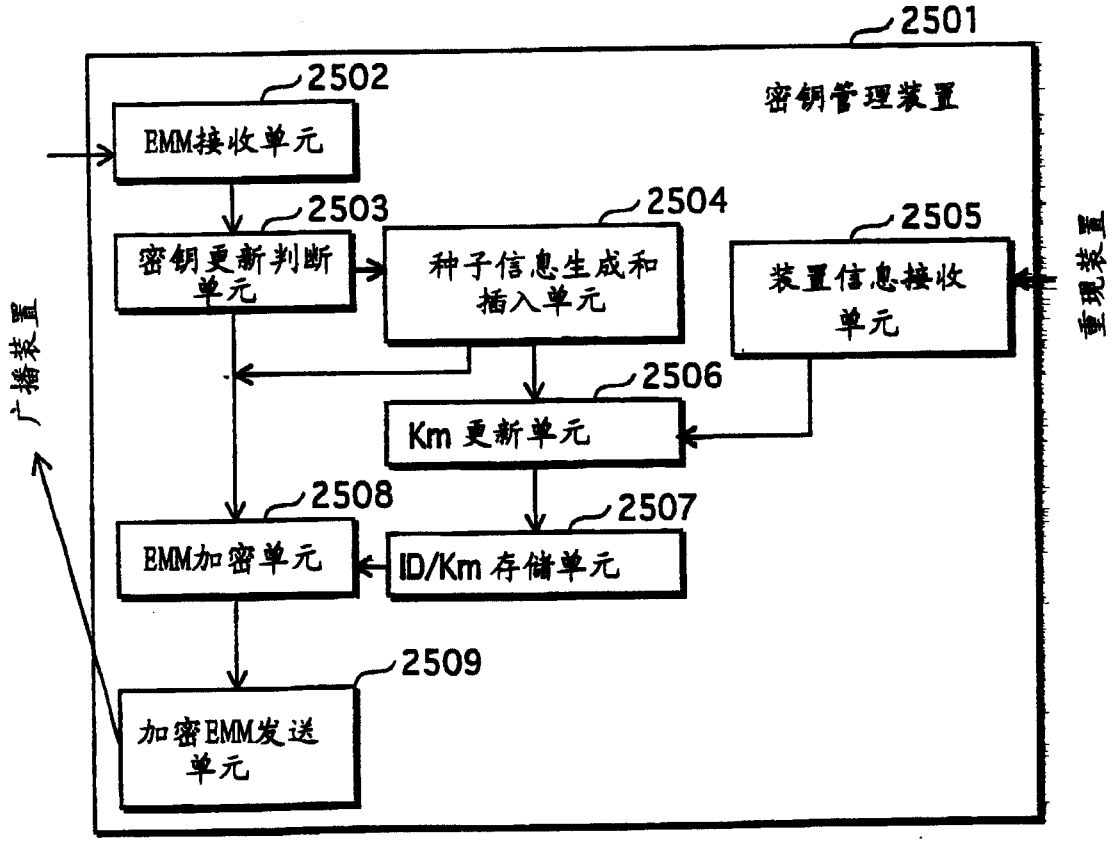

2501
密钥管理装置
2502
EMM接收单元
2503
密钥更新判断单元
2504
种子信息生成和插入单元
2505
装置信息接收单元
2506
Km 更新单元
2507
ID/Km 存储单元
2508
EMM加密单元
2509
加密EMM发送单元
广播装置
实现装置

图 25

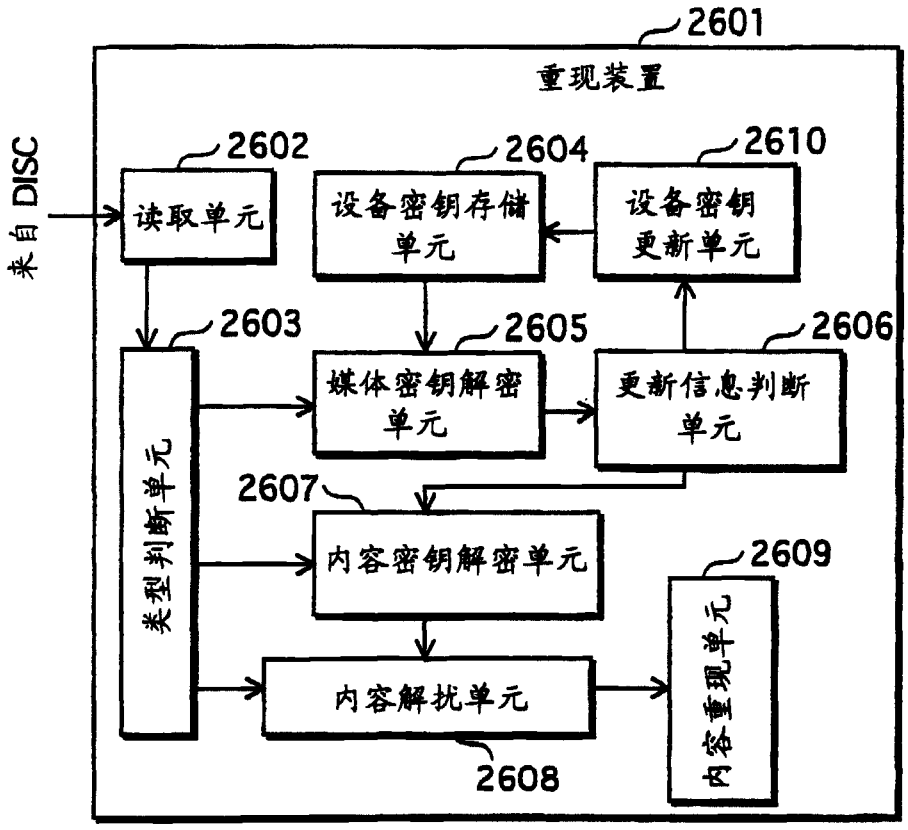

2601
重现装置
来自 DISC
2602
读取单元
2604
设备密钥存储单元
2610
设备密钥更新单元
2603
类型判断单元
2605
媒体密钥解密单元
2606
更新信息判断单元
2607
内容密钥解密单元
2609
内容重现单元
内容解扰单元
2608

图 26