

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 21/00 (2006.01)

H04L 29/06 (2006.01)



[12] 发明专利说明书

专利号 ZL 00813671.8

[45] 授权公告日 2006 年 3 月 29 日

[11] 授权公告号 CN 1248143C

[22] 申请日 2000.8.9 [21] 申请号 00813671.8

[30] 优先权

[32] 1999.8.10 [33] JP [31] 226406/99

[32] 1999.12.8 [33] JP [31] 349336/99

[86] 国际申请 PCT/JP2000/005339 2000.8.9

[87] 国际公布 WO2001/013358 日 2001.2.22

[85] 进入国家阶段日期 2002.3.29

[71] 专利权人 富士通株式会社

地址 日本神奈川县川崎市

共同专利权人 日本哥伦比亚株式会社

株式会社日立制作所

[72] 发明人 畑中正行 蒲田顺 畠山卓久

长谷部高行 小谷诚刚 古田茂树

穴泽健明 利根川忠明 日置敏昭

金森美和 堀吉宏

审查员 杨艳兰

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 马铁良 叶凯东

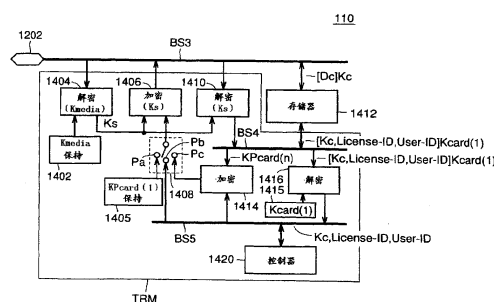
权利要求书 9 页 说明书 57 页 附图 43 页

[54] 发明名称

存储插件

[57] 摘要

存储插件(110)通过进行解密处理,从提供给数据总线 BS3 的数据抽出对话密钥 Ks。加密处理部(1406)根据对话密钥 Ks,将存储插件(110)的公开加密密钥 KPcard(1)加密并通过数据总线 BS3 提供给服务器。存储器(1412)从服务器接收并存入由每个存储插件都不同的公开加密密钥 KPcard(1)加密的许可密钥 Kc、许可 ID、用户 ID 等数据,从数据总线 BS3 接收并存入由许可密钥 Kc 加密了的加密内容数据 [Dc] Kc。



1. 一种接收并记录用于对加密内容数据进行解密的内容密钥用的存储插件，包括：

第1密钥保持部(1402)，保持将由对应上述存储插件预定的第1公开加密密钥加密的数据解密用的第1秘密解密密钥；

第1解密处理部(1404)，用于接收并解密处理在每次上述内容密钥的通信都被更新并发布、由第1公开加密密钥加密的第1公用密钥；

第2密钥保持部(1405)，用于保持上述每个存储插件固有的第2公开加密密钥；

第1加密处理部(1406)，用于将上述第2公开加密密钥根据上述第1公用密钥加密并输出；

第2解密处理部(1410)，用于接收由上述第2公开加密密钥加密、再由上述第1公用密钥加密的上述内容密钥，并根据上述第1公用密钥解密；

第1记忆部(1412)，用于接收并存入上述第2解密处理部的输出；

第3密钥保持部(1415)，保持将由上述第2公开加密密钥加密的数据解密用的第2秘密解密密钥；

第3解密处理部(1416)，用于根据存入上述第1记忆部的数据，通过上述第2秘密解密密钥，将上述内容密钥解密。

2. 权利要求1记载的存储插件，其中，

上述第1记忆部接收并存入可根据上述内容密钥解密的上述加密内容数据。

3. 权利要求2记载的存储插件，还包括：

控制部(1420)，用于按照外部指示的动作模式，控制上述存储插件的动作，

其中，

上述第1加密处理部由上述控制部控制，按照上述内容数据的再生动作的指示，接收来自上述第3解密处理部的上述内容密钥，并根据上述第1公用密钥进行加密并输出，

上述第1记忆部由上述控制部控制，按照上述内容数据的再生动作的指示，输出上述加密内容数据。

4. 权利要求 3 记载的存储插件，其中，

上述第 2 解密处理部，接收由上述第 2 公开加密密钥加密、再由上述第 1 公用密钥加密、并与上述内容密钥一起发布的许可信息数据，并根据上述第 1 公用密钥进行解密，

5 上述第 3 解密处理部，将由上述第 2 解密处理部提供的、关于第 1 公用密钥被解密关于上述第 2 公开加密密钥被加密的状态的上述许可信息数据解密，

还包括第 2 记忆部（1500），用于存入来自上述第 3 解密处理部的被解密的上述许可信息数据。

10 5. 权利要求 1 记载的存储插件，还包括：

第 4 密钥保持部（1440），保持对应上述存储插件预定的第 1 公开加密密钥，并可向外部输出。

6. 权利要求 5 记载的存储插件，其中，

15 上述第 1 记忆部，接收并存入可根据上述内容密钥解密的上述加密内容数据。

7. 权利要求 6 记载的存储插件，还包括：

控制部，用于按照外部指示的动作模式，控制上述存储插件的动作，

其中，

20 上述第 1 加密处理部，由上述控制部控制，按照上述内容数据的再生动作的指示，接收来自上述第 3 解密处理部的上述内容密钥，并根据上述第 1 公用密钥进行加密并输出，

上述第 1 记忆部，由上述控制部控制，按照上述内容数据的再生动作的指示，输出上述加密内容数据。

25 8. 权利要求 7 记载的存储插件，其中，

上述第 2 解密处理部接收由上述第 2 公开加密密钥加密、再由上述第 1 公用密钥加密、与上述内容密钥一起被发布的许可信息数据，根据上述第 1 公用密钥解密，

30 上述第 3 解密处理部将由上述第 2 解密处理部提供的、第 1 公用密钥被解密、上述第 2 公开加密密钥被加密的状态的上述许可信息数据解密，

还包含第 2 记忆部，用于存入来自上述第 3 解密处理部被解密的

上述许可信息数据。

9. 权利要求 1 记载的存储插件，还包括：

密钥数据生成部，生成第 2 公用密钥；

第 2 加密处理部，用于将上述第 2 公用密钥，通过上述第 1 公开
5 加密密钥加密，

其中，

被加密的上述第 2 公用密钥，被从上述存储插件发送到上述其它
存储插件。

10. 权利要求 2 或 6 记载的存储插件，包括：

10 安全区域（TRM），至少设有上述第 1 加密处理部、上述第 1 解密
处理部、上述第 2 解密处理部、上述第 3 解密处理部，且第三者不能
读出；

数据区域，设有上述第 1 记忆部，且第三者能够读出。

11. 权利要求 4 或 8 记载的存储插件，包括：

15 安全区域，至少设有上述第 1 加密处理部、上述第 1 解密处理部、
上述第 2 解密处理部、上述第 3 解密处理部、上述第 2 记忆部，且第
三者不能读出；

数据区域，设有上述第 1 记忆部，第三者能够读出。

12. 权利要求 2 或 6 记载的存储插件，其中，

20 上述第 1 记忆部，将上述加密内容数据附带的非加密数据同上述
加密内容数据一起接收并存入。

13. 一种用于接收并记录加密数据和将上述加密数据解密用的解
密信息数据的存储插件，包括：

第 1 记忆部（1412），存入上述加密数据；

25 第 1 密钥保持部（1442），为了能够通过公开认证密钥解密而将
对应上述存储插件预定的第 1 公开加密密钥和自身认证数据进行加密
保持，并能够向外部输出；

第 2 密钥保持部（1402），保持将由第 1 公开加密密钥加密的数
据解密用的第 1 秘密解密密钥；

30 第 1 解密处理部（1404），用于接收在每次上述解密信息数据的
通信都被更新并发送，由上述第 1 公开加密密钥加密的第 1 公用密钥，
并进行解密处理；

第3密钥保持部(1405)，用于保持上述每个存储插件固有的第2公开加密密钥；

对话密钥发生部(1432)，生成在每次上述解密信息数据通信都被更新的第2公用密钥；

5 第1加密处理部(1406)，用于将上述第2公开加密密钥和上述第2公用密钥，根据上述第1公用密钥，进行加密并输出；

第2解密处理部(1410)，用于将在外部由上述第2公开加密密钥加密、再由第2公用密钥加密的上述解密信息数据，根据上述第2公用密钥解密；

10 第2记忆部(1500)，存入作为上述第2解密处理部输出即由上述第2公开加密密钥加密的上述解密信息数据；

第4密钥保持部(1415)，保持将由上述第2公开加密密钥加密的数据解密用的第2秘密解密密钥；

第3解密处理部(1416)，用于根据上述第2秘密解密密钥，将
15 存入上述第2记忆部的数据解密，并抽出上述解密信息数据。

14. 权利要求13记载的存储插件，还包括：

第5密钥保持部(1450)，保持上述公开认证密钥；

第4解密处理部(1452)，解密并抽出为了能够通过上述公开认证密钥解密而加密的从外部提供的自身以外的第3公开加密密钥和自身以外的第2认证数据；
20

控制部(1420)，根据由上述第4解密处理部抽出的上述第2认证数据，进行认证处理，当不能认证时，禁止输出上述解密信息数据；

第2加密处理部(1430)，根据上述第3公开加密密钥，将在上述对话密钥生成部每次通信都更新的第2公用密钥，进行加密并输出；

25 第3加密处理部(1414)，用于根据来自外部的自身以外的固有的第4公开加密密钥，进行加密，

其中，

当有来自外部的解密信息数据的输出请求且上述控制部不禁止输出解密信息数据的场合，

30 i) 上述第2解密处理部再将由第2公用密钥加密的上述第1公用密钥或第4公开加密密钥及第1公用密钥进行解密输出；

ii) 当在上述第2解密处理部，上述第4公开加密密钥被抽出的

场合，上述第 3 解密处理部从记录于上述第 2 记忆部的数据抽出解密信息数据，上述第 3 加密处理部将上述由第 3 解密处理部抽出的解密信息数据，通过由上述第 2 解密处理部输出的第 4 公开加密密钥加密，进而，第 1 加密处理部将第 3 加密处理部的输出，根据在上述第 2 解密处理部抽出的第 2 公用密钥进行加密并输出；

iii) 当在上述第 2 解密处理部只抽出上述第 2 公用密钥的场合，上述第 3 解密处理部从存入上述第 2 记忆部的数据抽出解密信息数据，上述第 1 加密处理部将由上述第 3 解密处理部抽出的解密信息数据，根据由上述第 2 解密处理部抽出的第 2 公用密钥进行加密输出。

10 15. 权利要求 14 记载的存储插件，其中，

上述解密信息数据还包含访问控制数据，用于控制来自上述解密信息数据存储插件的输出，

还包括第 3 记忆部，上述第 3 解密处理部从由作为上述第 2 解密处理部的输出的第 2 公开加密密钥加密的上述解密信息数据，再抽出上述解密信息数据，

并且存入由上述第 3 解密处理部抽出的上述解密信息数据内的上述访问控制信息，

上述控制部，禁止根据存入上述第 3 记忆部的上述访问控制数据，输出解密信息数据。

20 16. 权利要求 15 记载的存储插件，其中，

上述存储插件的记录空间区分为：

安全区域，第三者不能读出、改写；

准安全区域，第三者能够读出，存入数据被施行存储插件固有的加密；

25 非安全区域，第三者能够读出及改写，

上述安全区域包含上述第 1、第 3 密钥保持部及第 3 记忆部，

上述准安全区域包含上述第 2 记忆部，

上述非安全区域包含第 1 记忆部。

17. 权利要求 16 记载的存储插件，其中，

30 上述准安全区域及上述非安全区域被配置在同一存储器上。

18. 一种用于接收并记录加密数据和将上述加密数据解密用的解密信息数据的存储插件，包括：

第 1 记忆部，存入上述加密数据；

第 1 密钥保持部，为了能够通过公开认证密钥解密而将对应上述存储插件预定的第 1 公开加密密钥和自身认证数据进行加密保持，并能够向外部输出；

5 第 2 密钥保持部，保持将由第 1 公开加密密钥加密的数据解密用的第 1 秘密解密密钥；

第 1 解密处理部，用于接收在每次上述解密信息数据的通信都被更新并发送，由上述第 1 公开加密密钥加密的第 1 公用密钥，并进行解密处理；

10 第 3 密钥保持部，用于保持上述每个存储插件固有的第 2 公开加密密钥；

对话密钥发生部，生成在每次上述解密信息数据通信都被更新的第 2 公用密钥；

第 1 加密处理部，用于将上述第 2 公开加密密钥和上述第 2 公用密钥，根据上述第 1 公用密钥，进行加密并输出；

15 第 2 解密处理部，用于将在外部由上述第 2 公开加密密钥加密、再由第 2 公用密钥加密的上述解密信息数据，根据上述第 2 公用密钥解密；

第 4 密钥保持部，保持将由上述第 2 公开加密密钥加密的数据解密的第 2 秘密解密密钥；

第 3 解密处理部，用于接收在外部由上述第 2 公开加密密钥加密的解密信息数据，由上述第 2 秘密解密密钥将上述解密信息数据解密；

第 2 记忆部，存入上述解密信息数据。

19. 权利要求 18 记载的存储插件，还包括：

25 第 4 密钥保持部，保持上述公开认证密钥；

第 4 解密处理部，解密并抽出为了能够通过上述公开认证密钥解密而加密的从外部提供的自身以外的第 3 公开加密密钥和自身以外的第 2 认证数据；

30 控制部，根据由上述第 4 解密处理部抽出的上述第 2 认证数据，进行认证处理，当不能认证时，禁止输出上述解密信息数据；

第 2 加密处理部，根据上述第 3 公开加密密钥，将在上述对话密钥生成部每次通信都更新的第 2 公用密钥，进行加密并输出；

第 3 加密处理部，用于根据来自外部的自身以外的固有的第 4 公开加密密钥，进行加密，

其中，

当从外部有解密信息数据的输出请求，且在上述控制部禁止输出解密信息数据的场合，

i) 上述第 2 解密处理部，再将在外部由第 2 公用密钥加密的上述第 1 公用密钥或第 4 公开加密密钥及第 1 公用密钥进行解密抽出；

ii) 当在上述第 2 解密处理部，上述第 4 公开加密密钥被抽出的场合，上述第 3 解密处理部将记录于上述第 2 记忆部的解密信息数据，由在上述第 2 解密处理部抽出的第 4 公开加密密钥进行加密，进而，第 1 加密处理部根据在上述第 2 解密处理部抽出的第 2 公用密钥，将第 3 加密处理部的输出进行加密并输出；

iii) 当在上述第 2 解密处理部只抽出上述第 2 公用密钥的场合，上述第 1 加密处理部根据在上述第 2 解密处理部抽出的第 2 公用密钥，将记录于上述第 2 记忆部的解密信息数据进行加密并输出。

20. 权利要求 19 记载的存储插件，其中，

上述解密信息数据还含有访问控制数据，用于控制来自上述解密信息数据存储插件的输出，

上述控制部根据存入上述第 2 记忆部的上述访问控制数据，禁止输出解密信息数据。

21. 权利要求 20 记载的存储插件，其中，

上述存储插件的记录空间区分为：

安全区域，第三者不能读出、改写；

非安全区域，第三者能够读出、改写，

上述安全区域包含上述第 1 及第 3 密钥保持部及第 2 记忆部，上述非安全区域包含上述第 1 记忆部。

22. 一种用于接收并记录加密数据和将上述加密数据解密用的解密信息数据的存储插件，包括：

第 1 密钥保持部，为了能够通过公开认证密钥解密而将对应上述存储插件预定的第 1 公开加密密钥和自身认证数据进行加密保持，并能够向外部输出；

第 2 密钥保持部，保持将由第 1 公开加密密钥加密的数据解密用

的第1秘密解密密钥；

第1解密处理部，用于接收在每次上述解密信息数据的通信都被更新并发送，由上述第1公开加密密钥加密的第1公用密钥，并进行解密处理；

5 第3密钥保持部，用于保持上述每个存储插件固有的第2公开加密密钥；

对话密钥发生部，生成在每次上述解密信息数据通信都被更新的第2公用密钥；

第1加密处理部，用于将上述第2公开加密密钥和上述第2公用密钥，根据上述第1公用密钥，进行加密并输出；

第2解密处理部，用于将在外部由上述第2公开加密密钥加密、再由第2公用密钥加密的上述解密信息数据，根据上述第2公用密钥解密；

第4密钥保持部，保持将由上述第2公开加密密钥加密的数据解密的第2秘密解密密钥；

第3解密处理部，用于接收在外部由上述第2公开加密密钥加密的解密信息数据，由上述第2秘密解密密钥将上述解密信息数据解密；
记忆部（1500），存入上述解密信息数据。

23. 权利要求22记载的存储插件，还包括：

20 第4密钥保持部，保持上述公开认证密钥；

第4解密处理部，解密并抽出为了能够通过上述公开认证密钥解密而加密的从外部提供的自身以外的第3公开加密密钥和自身以外的第2认证数据；

控制部，根据由上述第4解密处理部抽出的上述第2认证数据，
25 进行认证处理，当不能认证时，禁止输出上述解密信息数据；

第2加密处理部，根据上述第3公开加密密钥，将在上述对话密钥生成部每次通信都更新的第2公用密钥，进行加密并输出；

第3加密处理部，用于根据来自外部的自身以外的固有的第4公开加密密钥，进行加密，

30 其中，

当从外部有解密信息数据的输出请求，且在上述控制部禁止输出解密信息数据的场合，

i) 上述第 2 解密处理部，再将在外部由第 2 公用密钥加密的上述第 1 公用密钥或第 4 公开加密密钥及第 1 公用密钥进行解密抽出；

ii) 当在上述第 2 解密处理部，上述第 4 公开加密密钥被抽出的场合，上述第 3 加密处理部将记录于上述记忆部的解密信息数据，由
5 在上述第 2 解密处理部抽出的第 4 公开加密密钥进行加密，进而，第 1 加密处理部根据在上述第 2 解密处理部抽出的第 2 公用密钥，将第 3 加密处理部的输出进行加密并输出；

iii) 当在上述第 2 解密处理部只抽出上述第 2 公用密钥的场合，上述第 1 加密处理部根据在上述第 2 解密处理部抽出的第 2 公用密钥，
10 将记录于上述记忆部的解密信息数据进行加密并输出。

24. 权利要求 23 记载的存储插件，其中，

上述解密信息数据还含有访问控制数据，用于控制来自上述解密信息数据存储插件的输出，

上述控制部根据存入上述记忆部的上述访问控制数据，禁止输出
15 解密信息数据。

25. 权利要求 24 记载的存储插件，其中，

上述存储插件的记录空间区分为：

安全区域，第三者不能读出、改写；

非安全区域，第三者能够读出、改写，

20 上述安全区域包含上述第 1 及第 3 密钥保持部及记忆部。

存储插件

5 技术领域

本发明涉及一种存储插件，其在向便携式电话等的终端发布信息用的信息发布系统中，使针对被拷贝的信息的版权保护成为可能。

现有技术

10 近年来，由于因特网等信息通信网等的进步，各用户利用所使用的便携式电话等面向个人的终端，能够容易地访问网络信息。

在这种信息通信中，通过数字信号传送信息。因而，比如各个人用户拷贝上述那样的信息通信网中传送的音乐或影像信息的场合，也几乎不会因这种拷贝使音质或画质变差，能够进行信息的拷贝。

15 因此，在这种信息通信网上传输音乐信息或图像信息等存在版权的作品的场合，如果不采取适当保护版权的办法，显然可能会侵犯版权者的权利。

另一方面，如果把版权保护作为最优先的目的，不能通过急剧扩大的数字信息通信网进行著作物数据的发布，基本上反而对复制著作
20 时可能收取一定版权费的版权者也没有好处。

在这里，不是通过上述那样的数字信息通信网进行发布，以记录数字信息的记录媒体为例考虑一下，关于通常销售的记录了音乐信息的CD（小型光盘），从CD向光磁盘（MD等）拷贝音乐数据，只要限于个人使用该拷贝的音乐，原则上可以自由进行。但是，进行数字录
25 音等的个人用户要支付数字录音机本身或MD等媒体货款中的一定额，间接作为对版权者的补偿费。

而且，从CD向MD拷贝数字信号的音乐信息的场合，鉴于这些信息几乎是没有因为拷贝而变差的数字信息，从1个MD再向其它MD作为数字信息拷贝音乐数据由于保护版权者而在设备结构上是不行
30 的。

即，现状是，能够自由进行从数字记录媒体的CD向MD的拷贝，但是不能进行从可记录的MD向MD的拷贝。

从这一情况看,通过数字信息通信网向公众发布音乐信息或图像信息,其本身就是受到版权者的公众发送权限制的行为,因此,为了保护版权,需要采取充分的措施。

5 这种场合,当然需要防止本来无接收权的用户接收通过信息通信网向公众发送的著作物数据,即使有接收权的用户接收的场合,还要防止随便复制接收的著作。

发明内容

10 本发明的目的是提供一种信息发布系统中的存储插件,该信息发布系统在通过信息通信网如便携式电话等信息通信网发布著作物数据的场合,只是有正当访问权的用户方可接收这种信息。

该发明的其它目的是提供一种信息发布系统中的存储插件,该信息发布系统能够防止所发布的著作物数据未经版权者许可的复制。

15 为了达到相关目的,本专利发明相关的接收并记录加密内容数据用的存储插件,包括:第1密钥保持部、第1解密处理部、第2密钥保持部、第1加密处理部、第2解密处理部、第1记忆部、第3密钥保持部和第3解密处理部。

第1密钥保持部,保持将由对应存储插件预定的第1公开加密密钥所加密的数据进行解密用的第1秘密解密密钥。

20 第1解密处理部,接收并解密处理在每次加密内容数据的通信都被更新并发布、由第1公开加密密钥加密的第1公用密钥。

第2密钥保持部,保持每个存储插件都不同的第2公开加密密钥。第1加密处理部,根据第1公用密钥,将第2公开加密密钥加密并输出。

25 第2解密处理部,接收由第2公开加密密钥加密、再由第1公用密钥加密的内容密钥,并根据第1公用密钥进行解密。第1记忆部接收并存入第2解密处理部的输出。第3密钥保持部保持将由第2公开加密密钥加密的数据进行解密用的第2秘密解密密钥。第3解密处理部,根据存入第1记忆部的数据,由第2秘密解密密钥将内容密钥解
30 密。

从本发明的另一个方面来看,接收并记录加密数据和解密加密数据用的解密信息数据用的存储插件,包含:第1记忆部、第1密钥保

持部、第2密钥保持部、第1解密处理部、第3密钥保持部、对话密钥发生部、第1加密处理部、第2解密处理部、第2记忆部、第4密钥保持部和第3解密处理部。

第1记忆部存入加密数据。第1密钥保持部，为了能够通过公开认证密钥解密，将对应存储插件预定的第1公开加密密钥和自身的认证数据加密、保持，并能够对外部输出。

第2密钥保持部，保持对由第1公开加密密钥加密的数据进行解密处理用的第1秘密解密密钥。第1解密处理部，接收在每次解密信息数据的通信都被更新并发送，由第1公开加密密钥加密的第1公用密钥，并进行解密处理。

第3密钥保持部，保持每个存储插件都不同的第2公开加密密钥。

对话密钥发生部，生成在每次解密信息数据通信都被更新的第2公用密钥。第1加密处理部根据第1公用密钥，将第2公开加密密钥和第2公用密钥加密并输出。第2解密处理部，将在外部由第2公开密码密钥加密、再根据第2公用密钥加密的解密信息数据根据第2公用密钥解密。

第2记忆部，存入作为第2解密处理部的输出即由第2公开密码密钥加密的解密信息数据。第4密钥保持部保持将由第2公开加密密钥加密的数据解密用的第2秘密解密密钥。第3解密处理部，根据第2秘密解密密钥将存入第2记忆部的数据解密，并抽出解密信息数据。

从本发明的再一个方面来看，接收并记录加密数据和加密数据解密密用的解密信息数据用的存储插件，包含：第1记忆部、第1密钥保持部、第2密钥保持部、第1解密处理部、第3密钥保持部、对话密钥发生部、第1加密处理部、第2解密处理部、第4密钥保持部、第3解密处理部和第2记忆部。

第1记忆部存入加密数据。第1密钥保持部，为了能够通过公开认证密钥解密，将对应存储插件预定的第1公开加密密钥和自身的认证数据加密、保持，并能够对外部输出。

第2密钥保持部，保持对由第1公开加密密钥加密的数据进行解密处理用的第1秘密解密密钥。第1解密处理部接收在每次解密信息

数据的通信都被更新并发送，由第1公开加密密钥加密的第1公用密钥，并进行解密处理。第3密钥保持部，保持每个存储插件都不同的第2公开加密密钥。

5 对话密钥发生部，生成在每次解密信息数据通信都被更新的第2公用密钥。第1加密处理部根据第1公用密钥，将第2公开加密密钥和第2公用密钥加密并输出。

第2解密处理部，将在外部由第2公开密码密钥加密、再根据第2公用密钥加密的解密信息数据根据第2公用密钥解密。

10 第4密钥保持部，保持将由第2公开加密密钥加密的数据进行解密处理用的第2秘密解密密钥。

第3解密处理部，接收在外部由第2公开加密密钥加密的解密信息数据，由第2秘密解密密钥将解密信息数据解密。第2记忆部，存入解密信息数据。

15 因而，根据本发明，其结构由于是只有正式用户才能接收内容数据并存入存储器中，而且让他人拷贝曾存入存储插件中的数据的情况，为了该他人在可以再生的状态下移植数据，在发送源不能再生数据，因此，可以防止因无限制的拷贝，而使版权蒙受不应有的侵犯。

附图说明

20 图1是概略说明本发明的信息发布系统整体结构用的概念图。

图2是集中说明图1所示信息发布系统中使用的通信用密钥数据（Key data）等特性的图。

图3是表示图1所示内容服务器10结构的概略框图。

图4是说明图1所示便携式电话机100结构用的概略框图。

25 图5是说明图4所示存储插件110结构用的概略框图。

图6是说明在图1及图3～图5说明过的数据发布系统中发布模式用的流程图。

图7是说明将实施例1的加密内容数据解密并作为音乐数据输出的再生模式的流程图。

30 图8是说明在2个存储插件间内容数据及密钥数据等移动的模式用的流程图。

图9是说明加密的内容数据复制模式用的流程图。

图 10 是说明本发明实施例 2 的存储插件 130 结构用的概略框图。

图 11 是说明存储插件 130 移动模式用的流程图。

图 12 是说明本发明实施例 3 的存储插件 140 结构用的概略框图。

图 13 是说明使用图 12 说明过的存储插件 140 的发布模式用的流程图。

图 14 是说明将实施例 3 的加密内容数据解密并作为音乐数据输出的再生模式的流程图。

图 15 是说明在 2 个存储插件间，内容数据及密钥数据等移动处理用的流程图。

图 16 是说明加密的内容数据复制模式用的流程图。

图 17 是说明将实施例 3 变形例的加密内容数据解密并作为音乐数据输出的再生模式的流程图。

图 18 是说明本发明实施例 4 的存储插件 150 结构用的概略框图。

图 19 是说明存储插件 150 移动模式用的流程图，是与实施例 2 的图 11 的对比图。

图 20 是说明本发明实施例 5 的存储插件 160 结构用的概略框图。

图 21 是说明使用图 20 说明过的存储插件 160 的发布模式用的流程图。

图 22 是说明将实施例 5 的加密内容数据解密并作为音乐数据输出的再生模式用的流程图。

图 23 是说明在 2 个存储插件间内容数据及密钥数据等移动模式用的流程图。

图 24 是说明本发明实施例 6 的存储插件 170 结构用的概略框图。

图 25 是说明存储插件 170 移动模式用的流程图。

图 26 是说明实施例 7 的便携式电话机 101 结构用的概略框图。

图 27 是表示对应于实施例 7 的存储插件 180 的内容服务器 11 结构的概略框图。

图 28 是说明本发明实施例 7 的存储插件 180 结构用的概略框图。

图 29 是说明使用本发明实施例 7 的存储插件 180 的发布模式用的流程图。

5 图 30 是说明将实施例 7 的加密内容数据解密并作为音乐数据输出的再生模式的流程图。

图 31 是说明在 2 个存储插件间、内容数据及密钥数据等移动模式用的流程图。

10 图 32 是说明实施例 8 中的便携式电话机 105 结构用的概略框图。

图 33 是表示对应于实施例 8 的存储插件 190 的内容服务器 12 结构的概略框图。

图 34 是说明本发明实施例 8 的存储插件 190 结构用的概略框图。

15 图 35 是表示实施例 8 的存储插件 190 记录区域配置的概略图。

图 36 是说明使用图 35 说明过的存储插件 190 的发布模式用的流程图。

图 37 是说明从保持于存储插件 190 的加密内容数据，作为音乐向外部输出用的再生模式的流程图。

20 图 38 是说明在实施例 8 的 2 个存储插件间移动处理用的流程图。

图 39 是表示实施例 9 的存储插件 200 结构的概略框图。

图 40 是表示实施例 9 的存储插件 200 记录区域配置的概略框图。

25 图 41 是说明使用图 38 说明过的存储插件 200 的发布模式用的流程图。

图 42 是说明从保持于存储插件 200 的加密内容数据，作为音乐向外部输出用的再生模式的流程图。

图 43 是说明在实施例 9 的 2 个存储插件间移动模式用的流程图。

30 实施方式

以下结合附图说明本发明的实施例。

[实施例 1]

图 1 是概略说明本发明的信息发布系统整体结构用的概念图。

另外，以下以通过便携式电话网，将音乐数据发布到各用户的数据发布系统结构为例进行说明，使用以下的说明只是为了更清楚起见，但本发明不限于这样的场合，也可以应用于将其它著作物数据如图像数据等著作物数据，通过其它信息通信网发布的场合。

参照图 1，管理存在版权的音乐信息的内容服务器 10，按照规定的密码方式将音乐数据（以下也称内容数据）加密之后，向信息发布的发布载波 20 即便便携式电话公司提供这样的加密数据。

发布载波 20 通过自己的便携式电话网将来自各用户的发布请求（发布 request）在内容服务器 10 中继。内容服务器 10 按照配线请求，将请求的内容数据进一步加密之后，通过发布载波 20 的便携式电话网，向各用户的便携式电话机发布。

在图 1 中，结构如下，便携式电话用户 1 的便携式电话机 100 中，接收由便携式电话 100 接收的加密的内容数据，对上述发送时进行的加密进行解密处理之后，存入向便携式电话机 100 中的音乐再生部（无图示）提供用的可装卸的存储插件 110。

进而，比如用户 1 可以通过连接于便携式电话机 100 的头戴耳机 130 等，听取这种再生内容数据的音乐。

以下，将这种内容服务器 10 与发布载波 20 合并，总称为音乐服务器 30。

另外，把从这种音乐服务器 30 向各便携式电话终端传送内容数据的处理叫作“发布”。

按照这种结构，首先，没有买正式存储插件即存储插件 110 的用户，接收再生来自音乐服务器 30 的发布数据是困难的。

而且，在发布载波 20 中，比如，在每次发布 1 首曲子的内容数据，都计数其度数，如果用户每次接收（下载）内容数据发生的版权费，都由发布载波 20 作为便携式电话的通话费收取，版权者容易确保版权费。

而且，这种内容数据发布的优点是，因为通过便携式电话网这一封闭系统进行，所以比因特网等开放系统，容易采取版权保护对策。

这时，比如有存储插件 112 的用户 2 通过自己的便携式电话机 102，可以直接从音乐服务器 30 接收内容数据的发布。但是，如果用

户 2 直接从音乐服务器 30 接收有相当信息量的内容数据等的话，有时接收需要较长时间。这种场合，如果能从已经接收了该内容数据发布的用户 1，拷贝该内容数据的话，会更加方便用户。

但是，从保护版权者权利的观点，不允许自由放任地拷贝内容数据
5 的系统结构。

在图 1 示例中，让用户 2 将用户 1 接收的内容数据与为能够再生内容数据本身及该内容数据所需信息一起拷贝的场合叫作内容数据的“移动”。这时，用户 1 为了让用户 2 拷贝每个再生所需信息（再生信息），进行信息移动后，要不可能在用户 1 进行内容数据的再生。
10 这里，所谓内容数据是指作为按照规定加密方式加密的加密内容数据被发布；所谓“再生信息”如后所述，是指可以将按照上述规定的加密方式所加密的内容数据进行解密的许可密钥和许可 ID 数据 License-ID、用户 ID 数据 User-ID 等许可信息。

对此，把在只有内容数据被加密的状态下，让用户 2 拷贝称为音乐信息的“复制”。
15

这时，在用户 2 的终端不能拷贝再生这种内容数据所需再生信息，因此，用户 2 只靠得到的加密的内容数据，不能再生音乐。从而，用户 2 在希望再生这种音乐时，需要重新从音乐服务器 30 接收能够再生内容数据用的再生信息的发布。然而，这时，因为可以只接收能再生用的信息发布即可，所以，与用户 2 直接从音乐服务器 30 接收所有发布的场合相比，能够在特别短的通话时间实现音乐再生。
20

例如，便携式电话机 100 及 102 是 PHS (Personal Handy Phone) (注册商标) 的场合，能够进行所谓收发两用模式通话，因此，利用这种功能，可以进行从用户 1 向用户 2 的一次性信息转移（移动）或者只转送（复制）加密的内容数据。
25

在图 1 所示的结构中，为了在用户侧能够再生加密发布的内容数据，系统所必须的是：第 1，发布通信中加密密钥（键）用的方式；第 2，发布数据加密方式本身；第 3，实现防止擅自拷贝如此发布的数据用的数据保护的结构。

图 2 是集中说明图 1 所示信息发布系统中所用通信用的密钥数据（密钥数据）等特性用图。
30

首先，在图 1 所示结构中，作为存储插件 100 内的数据处理管理

用密钥，是存储插件这一媒体种类中固有的，有对所有存储插件公用的秘密解密密钥 K_{media} 、每个存储插件都不同的公开加密密钥 $KP_{card}(n)$ 、由公开加密密钥 $KP_{card}(n)$ 加密的数据解密用的秘密解密密钥 $K_{card}(n)$ 。

- 5 在这里，秘密解密密钥 $K_{card}(n)$ 或秘密解密密钥 $KP_{card}(n)$ 表示中的自然数 n 表示各用户（存储插件）区别用号码。

即，由公开加密密钥 $KP_{card}(n)$ 加密的数据可以由各存储插件中存在的秘密解密密钥 $K_{card}(n)$ 解密。因而，在存储插件中的发布数据授受时，基本上，如后所述，使用 3 个密钥 K_{media} 、 $K_{card}(n)$ 、
10 $KP_{card}(n)$ 。

进而，作为存储插件外和存储插件间的数据授受中的秘密保持用的密码密钥，使用各媒体固有，即，所有存储插件公用的公开加密密钥 KP_{media} 、由公开加密密钥 KP_{media} 加密的数据解密用的秘密解密密钥 K_{media} 、以及按各次通信，如用户每次访问音乐服务器 30 而生
15 成的公用密钥 K_s 。

这里，公用密钥 K_s ，如上所述，可以作为用户对音乐服务器 30 每进行 1 次访问都发生的结构，也可以作为只要访问 1 次，对于多首曲子音乐信息都使用同一公用密钥的结构，另外，可以作为例如按每一乐曲名，变更该公用密钥之后，每次都向用户发布的结构。

- 20 以下，把这种通信单位或访问单位称为“对话”，把公用密钥 K_s 也称为“对话密钥”。

从而，公用密钥 K_s 在各通信对话有固有的值，在发布服务器或便携式电话机中管理。

另外，关于应发布的数据，首先，有将加密的内容数据解密的密钥即 K_c （以下称为许可密钥），由该许可密钥 K_c 加密的内容数据被
25 解密。还有含有能特定该内容数据的管理代码或限制再生次数等信息的许可 ID 数据 License-ID 和识别接收者用的用户 ID 数据 User-ID 等。这里，作为用户 ID 数据 User-ID，比如可以使用用户的电话号码等。

- 30 采用这种结构，可以按照许可 ID 数据 License-ID 中所含信息，进行版权者侧的版权保护方面的控制，另一方面，使用用户 ID 数据 User-ID，可以进行保护之类的控制，以保护用户的个人信息，如不

能让局外者知道用户的访问履历等。

发布数据中的内容数据 Dc, 如上所述, 比如是音乐数据, 把可由许可密钥 Kc 将该内容数据解密的数据称为加密内容数据[Dc]Kc。

在这里, [Y]X 表示是将数据 Y 变换为可由密钥 X 解密的密码的信息。

图 3 是表示图 1 所示内容服务器 10 结构的概略框图。内容服务器 10 包含发布信息数据库 304, 用于保持按照规定方式将内容数据(音乐数据)加密的数据或许可 ID 数据 License-ID 等发布信息; 计费数据库 302, 用于保持按照各用户对内容数据访问次数等的计费信息; 数据处理部 310, 用于通过数据总线 BS1 接收来自发布信息数据库 304 及计费数据库 302 的数据、进行规定的加密处理; 通信装置 350, 用于通过通信网, 在发布载波 20 与数据处理部 310 之间进行数据授受。

数据处理部 310 包含: 发布控制部 312, 用于按照数据总线 BS1 上的数据, 控制数据处理部 310 的动作; 对话密钥发生部 314, 用于由发布控制部 312 控制, 发生对话密钥 Ks; 加密处理部 316, 用于将由对话密钥发生部 314 生成的对话密钥 Ks, 通过公开加密密钥 KPmedia 加密, 提供给数据总线 BS1; 解密处理部 318, 通过通信装置 350 及数据总线 BS1, 接收各用户便携式电话机中由对话密钥 Ks 加密后发送的数据, 进行解密处理; 加密处理部 320, 用于使用由解密处理部 318 析取的公开加密密钥 KPcard(n), 将许可密钥或许可 ID 数据 License-ID 等数据控制于发布控制部 312, 加密; 加密处理部 322, 再由对话密钥 Ks 将加密处理部 320 的输出加密, 通过数据总线 BS1 提供给通信装置 350。

图 4 是说明图 1 所示便携式电话机 100 结构用的概略框图。

便携式电话机 100 包含天线 1102, 用于接收通过便携式电话网无线传送的信号; 收发信部 1104, 用于接收来自天线 1102 的信号, 变换为基本频带信号, 或调制来自便携式电话机的数据, 提供给天线 1102; 数据总线 BS2, 用于进行便携式电话机 100 各部分数据的授受; 控制器 1106, 用于通过数据总线 BS2, 控制便携式电话机 100 的动作; 触摸键部 1108, 用于向便携式电话机 100 提供来自外部的指示; 显示器 1110, 用于向用户提供从控制器 1106 等输出的信息, 作为视觉

信息；声音再生部 1112，用于在通常的通话模式中，根据通过数据总线 BS2 提供的接收数据，再生声音。

便携式电话机 100 还包含：可以装卸的存储插件 110，用于来自内容服务器 10 的内容数据进行解密处理；存储器接口 1200，用于
5 控制存储插件 110 与数据总线 BS2 之间的数据授受；对话密钥发生部 1502，在进行存储插件 110 与便携式电话机其它部分的数据授受时，通过随机值等发生将数据总线 BS2 上对话的数据加密用的对话密钥 Ks；加密处理部 1504，用于由公开加密密钥 KPmedia 将由对话密钥发生部 1502 生成的对话密钥加密，提供给数据总线 BS2；解密处理
10 部 1506，根据对话密钥发生部 1502 中生成的对话密钥 Ks，由对话密钥 Ks 将数据总线 BS2 上的数据解密、输出；音乐再生部 1508，用于接收解密处理部 1506 的输出，再生音乐信号；混合部 1510，用于接收音乐再生部 1508 的输出和声音再生部 1112 的输出，按照动作模式选择性输出；数字模拟变换部 1512，接收混合部 1510 的输出，变换
15 为向外部输出用的模拟信号；连接端子 1514，用于接收数字模拟变换部 1512 的输出，与头戴耳机 120 连接。

另外，为了简化说明，只记述本发明的内容数据发布方面的部分，关于便携式电话机原来备有的通话功能方面的部分，一部分省略。

20 图 5 是说明图 4 所示存储插件 110 结构用的概略框图。

存储插件 110 包含：数据总线 BS3，通过端子 1202，在与存储器接口 1200 之间授受信号；Kmedia 保持部 1402，用于保持秘密解密密钥 Kmedia；解密处理部 1404，从由存储器接口 1200 提供给数据总线 BS3 的数据，通过由秘密解密密钥 Kmedia 进行解密处理，抽出对话
25 密钥 Ks；KPcard(1) 保持部 1405，用于保持公开加密密钥 KPcard(1)；加密处理部 1406，用于根据由解密处理部 1404 抽出的对话密钥 Ks，将来自转换开关 1408 的输出加密，提供给数据总线 BS3；解密处理部 1410，将数据总线 BS3 上的数据，通过由解密处理部 1404 抽出的对话密钥 Ks 进行解密处理，提供给数据总线 BS4；存储器
30 1412，用于从数据总线 BS4 存入由每个存储插件都不同的公开加密密钥 KPcard(n) 加密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等数据，从数据总线 BS3 接收并存入由许可密钥 Kc

加密的加密内容数据[Dc] Kc.

转换开关 1408 有接点 Pa、Pb、Pc, 来自 KPCard(1) 保持部 1405 的加密密钥 KPCard(1) 被提供给接点 Pa, 数据总线 BS5 被提供给接点 Pb, 加密处理部 1414 的输出被提供给接点 Pc. 转换开关 1408 分别将提供给接点 Pa、Pb、Pc 的信号, 按照是“发布模式”、“再生模式”、“移动模式”某一动作模式, 选择性提供给加密处理部 1406.

存储插件 110 还包含: Kcard(1) 保持部 1415, 用于保持秘密解密密钥 Kcard(1) 的值; 解密处理部 1416, 将由公开加密密钥 KPCard(1) 加密, 且从存储器 1412 读出的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等 ([Kc, License-ID, User-ID]Kcard(1)) 进行解密处理, 提供给数据总线 BS5; 加密处理部 1414, 用于在数据移动处理等中, 从解密处理部 1410 接收对方的存储插件的公开加密密钥 KPCard(n), 根据该对方的公开加密密钥 KPCard(n), 将向数据总线 BS5 上输出的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等加密后, 向转换开关 1408 输出; 控制器 1420, 用于在与数据总线 BS5 之间, 接收许可 ID 数据 License-ID、用户 ID 数据 User-ID 等, 控制存储插件 110 的动作.

另外, 图 5 中实线围起的区域被置入模块 TRM, 目的是为了, 在存储插件 110 内, 当进行来自外部的不当开封处理等时, 借助于内部数据的清除或内部电路的破坏, 使第三者不能读出存在于该区域内的电路内的数据等.

这种模块一般叫作阻尼电阻模块 (Tamper Resistance Module).

当然, 也可以是包括存储器 1412 置入模块 TRM 内的结构. 但是, 图 5 所示结构优点是, 因为存储器 1412 中保持的数据都是加密了的数据, 因此第三者只用该存储器 1412 中的数据, 不可能再生音乐, 且在昂贵的阻尼电阻模块内, 没有必要设置存储器 1412, 因此, 可以降低制造成本.

图 6 是说明在图 1 及图 3~图 5 说明过的数据发布系统中发布模式用的流程图.

在图 6 中, 说明用户 1 使用存储插件 110, 从内容服务器 10 接收内容数据发布时的动作.

首先, 从用户 1 的便携式电话机 100 通过用户的密钥按钮操作

等, 对内容服务器 10 进行发布请求 (步骤 S100)。

在内容服务器 10 中, 按照该发布请求, 对话密钥发生部 314 生成对话密钥 Ks (步骤 S103)。

接着, 服务器内的加密处理部 316 通过公开加密密钥 KPmedia, 5 将对话密钥 Ks 进行加密处理, 提供给数据总线 BS1 (步骤 S104)。

通信装置 350 将来自加密处理部 316 的加密对话密钥 [Ks]Kmedia, 通过通信网向便携式电话机 100 的存储插件 110 发送 (步骤 S106)。

在存储插件 110 中, 将通过存储器接口 1200 提供给数据总线 BS3 10 的接收数据, 解密处理部 1404 通过由 Kmedia 保持部 1402 提供的秘密解密密钥 Kmedia 进行解密处理, 将对话密钥 Ks 解密、抽出 (步骤 S108)。

接着, 在发布模式中, 转换开关 1408 选择接点 Pa 关闭的状态, 因此, 加密处理部 1406 将通过接点 Pa, 由 KPcard (1) 保持部 1405 15 提供的公开加密密钥 KPcard (1) (用户 1 的存储插件中的公开加密密钥) 由对话密钥 Ks 加密, 提供给数据总线 BS3 (步骤 S110)。

便携式电话机 100 向内容服务器 10 输出由加密处理部 1406 加密的数据 [KPcard (1)] Ks (步骤 S112)。

在内容服务器 10, 解密处理部 318 通过对话密钥 Ks 将由通信装置 20 350 接收、提供给数据总线 BS1 的数据 [KPcard (1)] Ks 进行解密处理, 解密抽出公开加密密钥 KPcard (1) (步骤 S114)。

接着, 发布控制部 312 从发布信息数据库 304 取得许可密钥 Kc (步骤 S116), 且以发布信息数据库 304 等中保持的数据为基础, 生成许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等许可信息(25 步骤 S118)。

加密处理部 320 接收来自发布控制部 312 的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据, 通过由解密处理部 318 提供的公开加密密钥 KPcard (1) 进行加密处理(步骤 S120)。

加密处理部 322 接收由加密处理部 320 加密的数据, 再由对话密 30 钥 Ks 加密, 提供给数据总线 BS1 (步骤 S122)。

通信装置 350 向插件 110 发送由加密处理部 322 加密的数据 [[Kc, License-ID, User-ID]Kcard (1)]Ks。

在存储插件 110 中,解密处理部 1410 通过对话密钥 Ks 进行解密处理,抽出数据 [Kc, License-ID, User-ID]Kcard(1)(步骤 S126)、存入存储器 1412(步骤 S128)。

另一方面,内容服务器 10 从发布信息数据库 304 取得加密内容数据 [Dc]Kc,通过通信装置 350,发送给存储插件 110(步骤 S130)。

在存储插件 110 中,将接收的数据 [Dc]Kc 直接存入存储器 1412(步骤 S132)。

通过以上动作,存储插件 110 存入的内容数据变为可再生状态,因此,以下,把存储插件存入的内容数据变为可再生状态称为“存储插件 110 处于状态 SA”。

图 7 是说明在便携式电话机 100 内,从保持于存储插件 110 的加密内容数据,将内容数据解密,作为音乐向外部输出用的再生处理的流程图。

参照图 7,根据来自便携式电话机 100 的触摸键 1108 等的用户 1 的指示,向存储插件 110 输出再生请求(步骤 S200)。

存储插件 110 从存储器 1420 读出加密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等(步骤 S203),由秘密解密密钥 Kcard(1)将许可密钥 Kc、许可 ID 数据 License-ID 或用户 ID 数据 User-ID 进行解密处理(步骤 S204)。

控制器 1420 根据含于被解密的许可 ID 数据 License-ID 等的信息,判断是否是可解密数据的请求(步骤 S206),判断为可解密时,向便携式电话机控制器 1106 发送再生许可通知(步骤 S208)。

在便携式电话机 100 中,对话密钥发生电路 1502 生成对话密钥 Ks(步骤 S210),加密处理部 1504 通过公开加密密钥 KPmedia 将对话密钥 Ks 加密(步骤 S212),向数据总线 BS2 输出加密对话密钥 [Ks]Kmedia(步骤 S214)。

存储插件 110 通过数据总线 BS2,接收由便携式电话机 100 生成的加密对话密钥,由秘密解密密钥 Kmedia 解密、抽出(步骤 S216)。

接着,存储插件 110 通过抽出的对话密钥 Ks 将许可密钥 Kc 加密(步骤 S219),将加密许可密钥 [Kc]Ks 提供给数据总线 BS2(步骤 S220)。

便携式电话机 100 的解密处理部 1506 通过由对话密钥 Ks 进行解

密处理,取得许可密钥 Kc (步骤 S222)。

接着,存储插件 110 将加密内容数据 [Dc]Kc 从存储器 1412 读出,提供给数据总线 BS2 (步骤 S224)。

便携式电话机 100 的音乐再生部 1508 将加密内容数据 [Dc]Kc, 5 由抽出的许可密钥 Kc 进行解密处理 (步骤 S226), 再生内容数据, 提供给混合部 1510 (步骤 S228)。

另一方面,在步骤 S206 中,判断为控制器 1420 解密处理不可能时,存储插件 110 向便携式电话机 100 发送再生不许可通知 (步骤 S230)。

10 在步骤 S230 状态下,不能进行内容数据的再生,因此,以下将这种状态表述为“存储插件 110 处于状态 SB”。

图 8 是说明在 2 个存储插件间,内容数据及再生信息移动处理用的流程图。

首先,设定便携式电话机 100 为发送侧,便携式电话机 102 为接收侧。 15

便携式电话机 100 首先向自身侧的存储插件 110 和插入到接收侧的便携式电话机 102 的存储插件 112 输出移动请求 (步骤 S300)。

进一步,在便携式电话机 100 中,对话密钥发生电路 1502 生成对话密钥 Ks (步骤 S303), 加密处理部 1504, 使用公开加密密钥 KPmedia, 将对话密钥 Ks 加密 (步骤 S304), 将该加密对话密钥 [Ks]Kmedia, 通过数据总线 BS2, 传递给存储插件 110 同时, 例如在收发两用模式中, 通过天线 1102, 对装于便携式电话机 102 的存储插件 112 传递上述加密对话密钥 [Ks]Kmedia (步骤 S306)。 20

在存储插件 110 中, 由秘密解密密钥 Kmedia 解密抽出对话密钥 Ks (步骤 S318)。 25

同样,在插件 112 也是由秘密解密密钥 Kmedia 解密抽出对话密钥 Ks (步骤 S320), 再由对话密钥 Ks 将存储插件 112 的公开加密密钥 KPcard (2) 加密 (步骤 S322), 向存储插件 110 发送加密的数据 [KPcard (2)]Ks (步骤 S324)。

30 在存储插件 110 中, 将从存储插件 112 发送的加密数据由对话密钥 Ks 解密, 解密抽出存储插件 112 的公开加密密钥 KPcard (2) (步骤 S326)。

接着，在存储插件 110 中，从存储器 1412 读出由存储插件 110 的公开加密密钥 Kcard (1) 加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID (步骤 S328)。

接着，解密处理部 1416 通过秘密解密密钥 Kcard (1) 解密处理
5 许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID (步骤 S330)。

进一步，加密处理部 1414 通过解密处理部 1410 中抽出的插件 112 中的公开加密密钥 Kpcard (2)，将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 加密 (步骤 S332)。

10 由加密处理部 1414 加密的数据再通过转换开关 1408 (接点 Pc 关闭)，被提供给加密处理部 1406，加密处理部 1406 通过对话密钥 Ks 将数据 [Kc, License-ID, User-ID]Kcard (2) 加密 (步骤 S334)。

接着，存储插件 110 通过便携式电话机 100，向存储插件 112 发送加密的数据 [[Kc, License-ID, User-ID]Kcard (2)]Ks (步骤
15 S336)。

在存储插件 112 中，将从存储插件 110 发送的数据，通过解密处理部 1410，根据对话密钥 Ks 进行解密处理 (步骤 S338)，存入存储器 1412 (步骤 S340)。

另一方面，存储插件 110 再清除存储器 1412 内数据中的对应于
20 许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 的数据 (步骤 S342)。

接着，存储插件 110 从存储器读出加密内容数据 [Dc]Kc，向存储插件 112 发送 (步骤 S344)。

存储插件 112 将接收的加密内容数据直接存入存储器 1412 (步
25 骤 S346)。

一进行以上处理，在步骤 S342 中，许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等被从存储插件 110 清除，因此，存储插件 110 变成“状态 SB”。

另一方面，在存储插件 112 中，除加密内容数据以外，许可密钥、
30 许可 ID 数据 License-ID、用户 ID 数据 User-ID 等所有数据也都移动，因此存储插件 112 变成“状态 SA”。

图 9 是说明在图 1 所示信息发布系统中，从便携式电话机 100 向

便携式电话机 102 进行加密内容数据复制处理用的流程图。

参照图 9, 便携式电话机 100 向存储插件 110 及存储插件 112 输出复制请求 (步骤 S400)。

接着, 存储插件 110 从存储器 1412 读出加密内容数据 [Dc]Kc, 向存储插件 112 输出 (步骤 S402)。

在存储插件 112 中, 将从存储插件 110 发送的加密的内容数据直接记录于存储器 1412 (步骤 S404)。

一进行以上动作, 加密内容数据、许可密钥 Kc、用户 ID 数据 User-ID、许可 ID 数据 License-ID 等所有数据被保留于存储插件 110, 因此, 存储插件 110 处于再生可能状态即“状态 SA”。

另一方面, 存储插件 112 因为只有加密内容数据, 所以不能直接进行再生处理。因而, 此时, 存储插件 112 处于“状态 SB”。

存储插件 112 为了变成状态 SA, 需要重新从内容服务器 10 取得许可密钥 Kc、许可 ID 数据 License-ID 或用户 ID 数据 User-ID 等再生信息。

按照上述结构, 只有有存储插件的正式用户才能接收内容数据 (音乐数据) 存入存储器中, 且将曾存入存储插件中的数据让他人拷贝时, 该他人为在再生可能状态下移植数据, 在发送源, 变为不能再生数据的结构, 因此, 可以防止由于无限制拷贝侵犯版权。

另外, 在以上说明中, 来自内容服务器 10 的加密数据解密用电路结构为置入能在便携式电话机中装卸的存储插件内, 但, 例如也可以设置于便携式电话机内部。也可作为最常见的置入能在访问信息服务器的终端设备装卸的存储插件内的结构, 也可以事先置入该终端设备。

[实施例 2]

图 10 是说明本发明实施例 2 的存储插件 130 结构用的概略框图, 是与实施例 1 的图 5 的对比图。

与实施例 1 的存储插件 110 结构的不同点之一是, 存储插件 130 内设有对话密钥 Ks 生成用的对话密钥发生电路 1432, 且设有保持对应于存储插件这一媒体的公开加密密钥 KPmedia 值的 KPmedia 保持部 1440。相应地, 存储插件 130 的结构包含: 加密处理部 1430, 用于由对话密钥发生电路 1432 生成的对话密钥 Ks, 通过公开加密密钥

KPmedia 加密, 提供给数据总线 BS3; 转换开关 1434, 用于接收来自对话密钥发生电路 1432 的输出和解密处理部 1404 的输出, 选择性提供给加密处理部 1406 和解密处理部 1410.

转换开关 1434 有接点 Pd、Pe、Pf, 向接点 Pd、Pe 提供解密处理部 1404 的输出, 向接点 Pf 提供对话密钥发生电路 1432 的输出. 转换开关 1434 分别将提供给接点 Pd、Pe、Pf 的信号, 按照动作模式是“发布模式”、“再生模式”、“移动模式”某一种, 选择性提供给加密处理部 1406 和解密处理部 1410.

其它结构与图 5 所示实施例 1 的存储插件 110 结构相同的同一部分附加同一符号, 其说明不重复.

存储插件 130 的动作与存储插件 110 的动作不同的是进行“移动”处理的场合.

图 11 是说明存储插件 130 的移动处理用的流程图, 是实施例 1 的图 8 的对比图.

参照图 11, 首先, 在图 11 中也设便携式电话机 100 是发送侧, 便携式电话机 102 是接收侧. 另外, 便携式电话机 102 也装有与存储插件 130 结构相同的存储插件 132.

便携式电话机 100 首先向自身侧的存储插件 130 和插入接收侧便携式电话机 102 的存储插件 132, 输出移动请求 (步骤 S300).

进而, 在便携式电话机 100 中, 存储插件 130 内的对话密钥发生电路 1432 生成对话密钥 Ks (步骤 S312), 使用公开加密密钥 KPmedia, 加密处理部 1430 将对话密钥 Ks 加密 (步骤 S314), 例如, 在收发两用模式中, 通过天线 1102, 将加密的对话密钥 Ks 传递给插件 132 (步骤 S316).

在存储插件 132 中, 解密处理部 1404 通过秘密解密密钥 Kmedia 将对话密钥 Ks 解密抽出 (步骤 S320), 再由对话密钥 Ks 将存储插件 132 的公开加密密钥 KPcard(2) 加密 (步骤 S322), 向存储插件 110 发送加密的数据 [KPcard(2)]Ks (步骤 S324).

在存储插件 110 中, 由对话密钥 Ks 将从存储插件 112 发送的加密数据解密, 解密抽出存储插件 112 的公开加密密钥 KPcard(2) (步骤 S326).

以下处理, 基本与图 8 说明过的实施例 1 的移动处理相同, 因此,

其说明不重复。

一进行上述处理，在步骤 S342 中，许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等被从插件 130 中清除，因此，存储插件 130 变为“状态 SB”。

- 5 另一方面，在存储插件 132 中，除加密内容数据以外，许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等再生信息也被移动，因此，存储插件 132 变为“状态 SA”。

采用上述结构，增加了实施例 1 的存储插件的效果，例如不通过有上述那样的对话密钥发生电路 1502 的便携式电话终端，通过可连接存储插件与存储插件的接口设备，也能够进行从存储插件 130 向存储插件 132 的数据移动，进一步方便了用户。

[实施例 3]

图 12 是说明本发明实施例 3 存储插件 140 结构用概略框图，是实施例 1 的图 5 的对比图。

- 15 与实施例 1 存储插件 110 的结构的不同点是存储插件 140 内设有可授受控制器 1420 和数据的寄存器 1500。

其它结构与图 5 所示实施例 1 的存储插件 5 的结构相同，因此，同一部分附加相同符号，其说明不重复。

图 13 是说明使用图 12 说明过的存储插件 140 的发布模式用的流程图。

在图 13 中也是说明用户 1 使用存储插件 140，从内容服务器 10 接收内容数据发布时的动作。

首先，从服务器 1 的便携式电话机 100，通过用户触摸键 1108 的操作等，对内容服务器 10 进行发布请求（步骤 S100）。

- 25 在内容服务器 10 中，按照该发布请求，对话密钥发生部 314 生成对话密钥 Ks（步骤 S103）。

接着，内容服务器 10 内的加密处理部 316 通过公开加密密钥 KPmedia，将对话密钥 Ks 进行加密处理，提供给数据总线 BS1（步骤 S104）。

- 30 通信装置 350 通过通信网，向便携式电话机 100 的存储插件 140 发送来自加密处理部 316 的加密内容数据 [Ks]Kmedia（步骤 S106）。

在存储插件 140 中，解密处理部 1404 将通过存储器接口 1200 提

供给数据总线 BS3 的接收数据, 经由秘密解密密钥 Kmedia 解密处理, 解密抽出对话密钥 Ks (步骤 S108)。

接着, 在发布模式中, 转换开关 1408 选择接点 Pa 关闭的状态, 因此, 加密处理部 1406 将由接点 Pa 提供的公开加密密钥 KPcard(1) (用户 1 的存储插件中的公开加密密钥), 由对话密钥 Ks 加密, 提供供给数据总线 BS3。

便携式电话机 100 将由加密处理部 1406 加密的数据 [KPcard(1)]Ks, 向内容服务器 10 输出 (步骤 S112)。

在内容服务器 10 中, 解密处理部 318 将通过通信装置 350 接收、提供供给数据总线 BS1 的数据 [KPcard(1)]Ks, 由对话密钥 Ks 进行解密处理, 解密抽出公开加密密钥 KPcard(1) (步骤 S114)。

接着, 发布控制部 312 从发布信息数据库 304 取得许可密钥 Kc (步骤 S116) 且以保持于发布信息数据库 304 等的数据为基础, 生成许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据 (步骤 S118)。

加密处理部 320 接收来自发布控制部 312 的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据, 通过由解密处理部 318 提供的公开加密密钥 KPcard(1) 进行加密处理 (步骤 S120)。

加密处理部 322 接收由加密处理部 320 加密的数据, 再由对话密钥 Ks 加密, 提供供给数据总线 BS1 (步骤 S122)。

通信装置 350 向插件 140 发送由加密处理部 322 加密的数据 [[Kc, License-ID, User-ID]Kcard(1)]Ks。

在存储插件 140 中, 解密处理部 1410 通过对话密钥 Ks 进行解密处理, 抽出数据 [Kc, License-ID, User-ID]Kcard(1) (步骤 S126), 存入存储器 1412 (步骤 S128)。

进而, 在存储插件 140 中, 解密处理部 1416 将存入存储器 1412 中的数据 [Kc, License-ID, User-ID]Kcard(1) 解密, 控制器 1420 将被解密的数据 License-ID、User-ID 存入寄存器 1500 (步骤 129)。

另一方面, 服务器 30 从发布信息数据库 304 取得加密内容数据 [Dc]Kc, 通过通信装置 350 发送到存储插件 140 (步骤 S130)。

在存储插件 140 中, 将接收的加密内容数据 [Dc]Kc 直接存入存储器 1412 (步骤 S132)。

通过上述动作，存储插件 140 变为可再生音乐信息状态。

图 14 是说明在便携式电话机 100 内，从保持于存储插件 140 的加密内容数据，将音乐信息解密，作为音乐向外部输出用的再生处理的流程图。

- 5 参照图 14，根据来自便携式电话机触摸键 1108 等的用户 1 的指示，向存储插件 140 输出再生请求（步骤 S200）。

在存储插件 140 中，控制器 1420 从寄存器 1500 读出许可 ID 数据 License-ID、用户 ID 数据 User-ID 等（步骤 S205）。

- 10 控制器 1420 根据许可 ID 数据 License-ID 等中所含信息，判断是否是可解密的数据的请求（步骤 S206），判断为可解密の場合，向便携式电话机的控制器 1106 发送再生许可通知（步骤 S208）。

- 在便携式电话机 100 中，对话密钥发生电路 1502 生成对话密钥 Ks（步骤 S210），加密处理部 1504 通过公开加密密钥 KPmedia 将对话密钥 Ks 加密（步骤 S212），向数据总线 BS2 输出加密对话密钥
15 [Ks]Kmedia（步骤 S214）。

存储插件 140 通过数据总线 BS2，接收由便携式电话机生成的加密对话密钥 [Ks]Kmedia，由公开加密密钥 Kmedia 解密，抽出对话密钥 Ks（步骤 S216）。

- 接着，存储插件 140 从存储器 1412 读出加密的数据 [Kc, License-ID, User-ID]Kcard(1)，解密处理部 1416 解密，抽出许可密钥 Kc（步骤 S218）。

接着，通过抽出的对话密钥 Ks 将许可密钥 Kc 加密（步骤 S219），将加密许可密钥 [Kc]Ks 提供给数据总线 BS2（步骤 S220）。

- 便携式电话机 100 的解密处理部 1506 通过由对话密钥 Ks 进行解密处理，取得许可密钥 Kc（步骤 S222）。

接着，存储插件 140 从存储器 1412 读出加密内容数据 [Dc]Kc，提供给数据总线 BS2（步骤 S224）。

- 便携式电话机的音乐再生部 1508 将加密内容数据 [Dc]Kc，通过抽出的许可密钥 Kc 进行解密处理（步骤 S226），再生内容数据，提供给混合部 1510（步骤 S228）。

另一方面，在步骤 S206 中，判断为控制器 1420 不可能进行解密处理时，存储插件 140 向便携式电话机 100 发送不许可再生通知（步

骤 S230)。

在步骤 S230 的状态下, 存储插件 140 处于状态 SB。

图 15 是说明在 2 个存储插件间, 内容数据及密钥数据等移动处理用的流程图。

- 5 首先, 设定便携式电话机 100 为发送侧, 便携式电话机 102 为接收侧。另外, 便携式电话机 102 也装有与存储插件 140 结构相同的存储插件 142。

便携式电话机 100 首先向自身侧的存储插件 140 和插入接收侧便携式电话机 102 的存储插件 142 输出移动请求 (步骤 S300)。

- 10 进而, 在便携式电话机 100 中, 对话密钥发生电路 1502 生成对话密钥 Ks (步骤 S303), 使用公开加密密钥 KPmedia, 加密处理部 1504 将对话密钥 Ks 加密 (步骤 S304), 通过数据总线 BS2, 传递给存储插件 140, 进一步, 比如在收发两用模式中, 通过天线 1102, 将加密的对话密钥 Ks 传递给存储插件 142 (步骤 S306)。

- 15 在存储插件 140 中, 由秘密解密密钥 Kmedia 解密抽出对话密钥 Ks (步骤 S318)。

- 同样, 在存储插件 142 中也是由秘密解密密钥 Kmedia 将对话密钥 Ks 解密抽出 (步骤 S320), 再由对话密钥 Ks 将插件 142 的公开加密密钥 KPcard (2) 加密 (步骤 S322), 向存储插件 140 发送加密的数据 [KPcard (2)]Ks (步骤 S324)。
- 20

在存储插件 140 中, 将从存储插件 142 发送的加密数据由对话密钥 Ks 解密, 解密抽出存储插件 142 的公开加密密钥 KPcard (2) (步骤 S326)。

- 接着, 在存储插件 140 中, 从存储器 1412 读出由存储插件 140 的公开加密密钥 Kcard (1) 加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID (步骤 S328)。
- 25

接着, 解密处理部 1416 通过秘密解密密钥 Kcard (1), 解密处理许可密钥 Kc、解密 ID 数据 License-ID、用户 ID 数据 User-ID (步骤 S330)。

- 30 控制器 1420 将这样被解密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 的值与寄存器 1500 内的数据值置换 (步骤 S331)。

进一步, 加密处理部 1414 通过在解密处理部 1410 抽出的存储插件 142 中的公开加密密钥 Kpcard(2), 将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 加密(步骤 S332)。

由加密处理部 1414 加密的数据通过转换开关 1408(接点 Pc 关闭), 再被提供给加密处理部 1406, 加密处理部 1406 通过对话密钥 Ks 将数据 [Kc, License-ID, User-ID]Kcard(2) 加密(步骤 S334)。

接着, 存储插件 140 通过便携式电话机 100, 向存储插件 142 发送加密的数据 [[Kc, License-ID, User-ID]Kcard(2)]Ks(步骤 S336)。

在存储插件 142 中, 将从存储插件 140 发送的数据, 通过解密处理部 1410, 根据对话密钥 Ks 进行解密处理, 存入存储器 1412(步骤 S339)。进一步, 在存储插件 142 中, 解密处理部 1416 根据秘密解密密钥 Kcard(2), 将数据 [Kc, License-ID, User-ID]Kcard(2) 解密, 将被解密的许可 ID 数据 License-ID、用户 ID 数据 User-ID 存入寄存器(步骤 S341)。

另一方面, 存储插件 140 再清除存入寄存器 1500 的许可 ID 数据 License-ID 及用户 ID 数据 User-ID(步骤 S343)。

接着, 存储插件 140 将加密内容数据 [Dc]Kc 从存储器读出, 向存储插件 142 发送(步骤 S344)。

存储插件 142 将接收的加密内容数据直接存入存储器 1412(步骤 S346)。

一进行上述处理, 在步骤 S343 中, 许可 ID 数据 License-ID 及用户 ID 数据 User-ID 被从存储插件 140 的寄存器 1500 中清除, 因此, 存储插件 140 变为“状态 SB”。

另一方面, 在存储插件 142 中, 除加密内容数据以外, 许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等所有数据也被移动, 因此, 存储插件 142 变为“状态 SA”。

图 16 是说明在图 12 所示存储插件 140 中, 从便携式电话机 100 向便携式电话机 102 进行加密内容数据复制处理用的流程图。

参照图 16, 便携式电话机 100 向存储插件 140 及存储插件 142 输出复制请求(步骤 S400)。

接着, 存储插件 140 将加密内容数据 [Dc]Kc 从存储器 1412 读出,

向存储插件 142 发送（步骤 S402）。

在存储插件 142 中，将由存储插件 140 发送的加密内容数据直接记录于存储器 1412（步骤 S404）。

一进行上述动作，被加密的内容数据、许可密钥 Kc、用户 ID 数据 User-ID、许可 ID 数据 License-ID 等所有数据被保留于存储插件 140，因此，存储插件 140 处于可再生状态即“状态 SA”。

另一方面，存储插件 142 只有加密内容数据，因此，不能直接进行再生处理。因而，此时，存储插件 142 处于“状态 SB”。

存储插件 142 为了变成状态 SA，需要重新从内容服务器 10 取得许可密钥 Kc、许可 ID 数据 License-ID 或用户 ID 数据 User-ID 等。

按照以上结构，与实施例 1 的存储插件 110 的效果相同，而且许可 ID 数据 License-ID 等被存入寄存器 1500，控制器 1420 可以参照它，因此，能够减少动作需要的处理量。

另外，在以上说明中，其结构为，来自内容服务器 10 的加密数据解密用电路置入可在便携式电话机装卸的存储插件内，但比如也可以设置于便携式电话机内部。更一般的结构是置入可在访问信息服务器的终端设备装卸的存储插件内，又可以事先置入该终端设备。

[实施例 3 的变形例]

实施例 3 的存储插件 140 的再生处理，采用判断由许可 ID 数据 License-ID 可否进行解密处理的结构。作为该许可 ID 数据 License-ID，其结构不仅包含乐曲名的特定信息，也包含再生次数的限制信息，还可以限制用户能够再生内容数据的次数。特别是在存储插件 140 中，是将许可 ID 数据 License-ID 保持于寄存器 1500 的结构，因此，正如下面的说明，每次进行再生处理，都容易更新许可 ID 数据 License-ID 的内容。

以下说明这种存储插件 140 的再生处理。

图 17 是说明在便携式电话机 100 内，从实施例 3 变形例的存储插件 140 中保持的加密内容数据，将内容数据解密，作为音乐向外部输出用的再生处理的流程图。

参照图 17，根据来自便携式电话机触摸键 1108 等的用户 1 的指示，向存储插件 140 输出再生请求（步骤 S200）。

在存储插件 140 中，控制器 1420 从寄存器 1500 读出许可 ID 数

据 License-ID、用户 ID 数据 User-ID 等（步骤 S205）。

控制器 1420 根据含于被解密的许可 ID 数据 License-ID 等的信息，判断由许可 ID 数据 License-ID 中的数据指定的内容数据（音乐数据）再生处理累计数是否超过可以再生次数的上限值（步骤 S206），
5 判断为没有超过可以再生次数时，向便携式电话机的控制器 1106 发送再生许可通知（步骤 S208）。

在便携式电话机 100 中，对话密钥发生电路 1502 生成对话密钥 Ks（步骤 S210），加密处理部 1504 通过秘密解密密钥 KPmedia 将对话密钥 Ks 加密（步骤 S212），加密对话密钥数据 [Ks]Kmedia 被输出到数据总线 BS2（步骤 S214）。
10

存储插件 140 通过数据总线 BS2，接收由便携式电话机生成的加密对话密钥 [Ks]Kmedia，由秘密解密密钥 Kmedia 解密，抽出对话密钥 Ks（步骤 S216）。

进一步，存储插件 140 按照进行再生处理，更新寄存器 1500 中的许可 ID 数据 License-ID 中的再生处理累计数方面的数据（步骤 217）。
15

接着，存储插件 140 从存储器 1412 读出被加密的数据 [Kc, License-ID, User-ID]Kcard (1)，解密处理部 1416 进行解密，抽出许可密钥 Kc（步骤 S218）。

接着，由抽出的对话密钥 Ks，将许可密钥 Kc 加密（步骤 S219），将加密许可密钥 [Kc]Ks 提供给数据总线 BS2（步骤 S220）。
20

便携式电话机 100 的解密处理部 1506 通过由对话密钥 Ks 进行解密处理，取得许可密钥 Kc（步骤 S222）。

接着，存储插件 140 将加密内容数据 [Dc]Kc 从存储器 1412 读出，提供给数据总线 BS2（步骤 S224）。
25

便携式电话机音乐再生部 1508 将加密内容数据 [Dc]Kc 由抽出的许可密钥 Kc 进行解密处理（步骤 S226），再生内容数据，提供给混合部 1510（步骤 S228）。

另一方面，在步骤 S206 中，判断为控制器 1420 不能进行解密处理时，存储插件 140 向便携式电话机 100 发送再生不许可通知（步骤 S230）。
30

按照上述结构，可以限制用户能再生内容数据的次数。

移动时, 关于限制再生信息内再生次数的许可 ID 数据 License-ID, 将记录于存储器 1412 的许可 ID 数据 License-ID, 变更为记录由寄存器 1500 每次再生时修正的再生次数的许可 ID 数据 License-ID, 构成新的再生信息。这样, 内容数据即使在存储插件间移动, 有再生次数限制的内容数据的再生次数也不会超过发布时规定的再生次数限制。

[实施例 4]

图 18 是说明本发明实施例 4 的存储插件 150 结构用的概略框图, 是实施例 2 的图 10 的对比图。

与实施例 2 的存储插件 130 结构的不同点是存储插件 150 内设有控制器 1420 和能授受数据的寄存器 1500。

其它结构与图 10 所示实施例 2 的存储插件 130 结构相同, 因此, 在同一部分附加相同符号, 其说明不重复。

图 19 是说明存储插件 150 移动模式用的流程图, 是实施例 2 的图 11 的对比图。

参照图 19, 首先, 在图 19 中也是, 设便携式电话机 100 为发送侧, 便携式电话机 102 为接收侧。另外, 在便携式电话机 102 中, 也装有与存储插件 150 相同结构的存储插件 152。

便携式电话机 100 首先向自身侧的存储插件 150 和插入接收侧便携式电话机 102 的存储插件 152 输出移动请求 (步骤 S300)。

进一步, 在便携式电话机 100 中, 存储插件 150 内的对话密钥发生电路 1432 生成对话密钥 K_s (步骤 S312), 使用公开加密密钥 KP_{media} , 加密处理部 1430 将对话密钥 K_s 加密 (步骤 S314), 比如, 在收发两用模式中, 通过天线 1102 将加密的对话密钥 K_s 传送到插件 152 (步骤 S316)。

在存储插件 152 中也是解密处理部 1404 通过秘密解密密钥 K_{media} , 将对话密钥 K_s 解密抽出 (步骤 S320), 再通过对话密钥 K_s 将存储插件 152 的公开加密密钥 $KP_{card}(2)$ 加密 (步骤 S322), 向存储插件 150 发送加密的数据 $[KP_{card}(2)]K_s$ (步骤 S324)。

在存储插件 150 中, 将从存储插件 152 发送的加密数据由对话密钥 K_s 解密, 解密抽出存储插件 152 的公开加密密钥 $KP_{card}(2)$ (步骤 S326)。

接着, 在存储插件 150 中, 从存储器 1412 读出由存储插件 150 的公开加密密钥 Kcard (1) 加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID (步骤 S328)。

接着, 解密处理部 1416 通过秘密解密密钥 Kcard (1), 对许可
5 密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 进行解密处理 (步骤 S330)。

控制器 1420 将这样解密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 的值与寄存器 1500 内的数据值置换 (步骤 S331)。

10 进一步, 加密处理部 1414 通过在解密处理部 1410 抽出的存储插件 152 中的公开加密密钥 KPcard (2), 将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 加密 (步骤 S332)。

由加密处理部 1414 加密的数据通过转换开关 1408 (接点 Pc 关闭), 再被提供给加密处理部 1406, 加密处理部 1406 通过对话密钥
15 Ks 将数据 [Kc, License-ID, User-ID]Kcard (2) 加密 (步骤 S334)。

接着, 存储插件 150 通过便携式电话机 100 向存储插件 152 发送加密的数据 [[Kc, License-ID, User-ID]Kcard (2)]Ks (步骤 S336)。

在存储插件 152 中, 将从存储插件 150 发送的数据, 通过解密处理部 1410, 根据对话密钥 Ks, 进行解密处理, 存入存储器 1412 (步骤 S339)。进一步, 存储插件 152 根据秘密解密密钥 Kcard (2),
20 将数据 [Kc, License-ID, User-ID]Kcard (2) 解密, 将解密的许可 ID 数据 License-ID、用户 ID 数据 User-ID 存入寄存器 1500 (步骤 S341)。

另一方面, 存储插件 150 再将存入寄存器 1500 的许可 ID 数据
25 License-ID 及用户 ID 数据 User-ID 清除 (步骤 S343)。

接着, 存储插件 150 从存储器读出加密内容数据 [Dc]Kc, 向存储插件 152 发送 (步骤 S344)。

存储插件 152 将秘密解密密钥直接存入存储器 1412 (步骤 S346)。

30 一进行上述处理, 在步骤 S342 中, 许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等被从存储插件 150 中清除, 因此, 存储插件 150 变为“状态 SB”。

另一方面，在存储插件 152 中，除加密的内容数据以外，许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等所有数据也被移动，因此，存储插件 152 变为“状态 SA”。

按照上述结构，实施例 2 的存储插件 130 效果增加，例如，从存储插件 150 向存储插件 152 的数据移动，不通过有上述那样对话密钥发生电路 1502 的便携式电话机，通过可连接存储插件与存储插件的接口设备也可以进行，因此有进一步方面用户的效果。

而且，许可 ID 数据 License-ID 等被存入寄存器 1500，控制器 1420 可以参照它，因此，能够减少动作所需处理量。

进而，也可以是限制用户能再生内容数据的次数的结构。

[实施例 5]

图 20 是说明本发明实施例 5 的存储插件 160 结构用的概略框图，是实施例 3 的图 12 的对比图。

以下，区别安装于便携式电话机 100 的存储插件 160 的公开加密密钥 KPmedia 和安装于便携式电话机 102 的存储插件 162 的公开加密密钥 KPmedia，分别把对于存储插件 160 的称为公开加密密钥 KPmedia (1)，把对于存储插件 162 的称为公开加密密钥 KPmedia (2)。

另外，按照此，可以将由公开加密密钥 KPmedia (1) 加密的数据解密，将与其非对称的秘密解密密钥称为秘密解密密钥 Kmedia (1)，可以将由公开加密密钥 KPmedia (2) 加密的数据解密，将与其非对称的秘密解密密钥称为秘密解密密钥 Kmedia (2)。

这样，通过区别媒体固有的公开加密密钥，通过以下的说明可以清楚，存在多种存储插件的场合或更一般地，存储插件以外的媒体作为系统选项存在的场合都可以对应。

参照图 20，本发明实施例 5 的存储插件 160 的结构与实施例 3 的存储插件 140 的结构的不同点是设有 KPmedia 保持部 1440，用于在存储插件 160 内保持对应于存储插件这一媒体的公开加密密钥 KPmedia(1) 的值、向数据总线 BS3 输出公开加密密钥 KPmedia(1)。

其它结构与图 12 所示实施例 3 的存储插件 140 的结构相同，因此，在同一部分附加相同符号，其说明不重复。

图 21 是说明使用图在 20 说明过的存储插件 160 的发布模式用的

流程图。

在图 21 还说明了用户 1 使用存储插件 160 接收来自内容服务器 10 的发布时的动作。

首先，从用户 1 的便携式电话机 100，通过用户触摸键的操作等进行发布请求（步骤 S100）。

在存储插件 160 中，按照该发布请求，从 KPmedia 保持部 1440 向内容服务器 10 发送公开加密密钥 KPmedia (1)（步骤 S101）。

内容服务器 10，一接收从存储插件 160 转送的发布请求及公开加密密钥 KPmedia (1)（步骤 S102），对话密钥发生部 314 生成对话密钥 Ks（步骤 S103）。

接着，内容服务器 10 内的加密处理部 316 通过公开加密密钥 KPmedia (1)，将对话密钥 Ks 进行加密处理，提供给数据总线 BS1（步骤 S104）。

通信装置 350 将来自加密处理部 316 的加密对话密钥 [Ks]Kmedia (1)，通过通信网，向便携式电话机 100 的存储插件 160 发送（步骤 S106）。

在存储插件 160 中，解密处理部 1404 将通过存储器接口 1200 提供给数据总线 BS3 的接收数据，通过由秘密解密密钥 Kmedia (1) 进行解密处理，将对话密钥 Ks 解密抽出（步骤 S108）。

以下处理与图 13 中说明过的实施例 3 的存储插件 140 的动作相同，因此，其说明不重复。

按照这样的结构，存储插件自身将公开加密密钥 KPmedia (1) 发送到传送对话密钥 Ks 侧（内容服务器 10）之后，能够接收发布，存储插件 160 变成可再生内容数据的状态。

图 22 是说明在便携式电话机 100 内，从保持于存储插件 160 的加密内容数据，将内容数据解密，作为音乐向外部输出用的再生处理的流程图。

参照图 22，根据来自便携式电话机触摸键 1108 等的用户 1 的指示，向存储插件 160 输出再生请求（步骤 S200）。

在存储插件 160 中，按照该再生请求，从 KPmedia 保持部 1440，向便携式电话机 100 发送公开加密密钥 KPmedia (1)（步骤 S201）。

便携式电话机 100，接收保持来自存储插件 160 的公开加密密钥

KPmedia (1) (步骤 S202)。

在存储插件 160 中, 控制器 1420 从寄存器 1500 读出许可 ID 数据 License-ID、用户 ID 数据 User-ID 等 (步骤 S205)。

5 控制器 1420 根据含于许可 ID 数据 License-ID 等的信息, 判断是否是可解密数据的请求 (步骤 S206), 判断为可解密时, 向便携式电话机的控制器 1106 发送再生许可通知 (步骤 S208)。

在便携式电话机 100 中, 对话密钥发生电路 1502 生成对话密钥 Ks (步骤 S210), 加密处理部 1504 通过公开加密密钥 KPmedia (1) 将对话密钥 Ks 加密 (步骤 S212), 向数据总线 BS2 输出加密对话密
10 钥 [Ks]Kmedia (1) (步骤 S214)。

存储插件 160 通过数据总线 BS2, 接收由便携式电话机生成且被加密的对话密钥 Ks, 由秘密解密密钥 Kmedia (1) 解密, 抽出对话密钥 Ks (步骤 S216)。

15 以下处理与图 14 中说明过的实施例 3 的存储插件 140 的动作相同, 因此, 其说明不重复。

按照这种结构, 存储插件自身将公开加密密钥 KPmedia (1) 发送到传送对话密钥 Ks 侧 (便携式电话机 100) 之后, 能够进行再生动作。

20 图 23 是说明在 2 个存储插件间进行内容数据及密钥数据等移动处理用的流程图。

首先, 设定便携式电话机 100 为发送侧, 便携式电话机 102 为接收侧。另外, 便携式电话机 102 中也装有与存储插件 160 同样结构的存储插件 162。

25 便携式电话机 100 首先向自身侧的存储插件 160 和插入到接收侧便携式电话机 102 的存储插件 162 输出移动请求 (步骤 S300)。

在存储插件 160 中, 向便携式电话机 100 发送公开加密密钥 KPmedia (1) (步骤 S301), 在存储插件 162 中, 向便携式电话机 100 发送公开加密密钥 KPmedia (2) (步骤 S301')。

30 便携式电话机 100 接收公开加密密钥 KPmedia (1) 及公开加密密钥 KPmedia (2) (步骤 302)。

进一步, 在便携式电话机 100 中, 对话密钥发生电路 1502 生成对话密钥 Ks (步骤 S303), 使用公开加密密钥 KPmedia (1) 及公

开加密密钥 $KP_{media}(2)$ ，加密处理部 1504 将对话密钥 K_s 加密（步骤 S304）。便携式电话机 100 通过数据总线 BS2，向存储插件 160 传递加密对话密钥 $[K_s]KP_{media}(1)$ ，进一步，比如，在收发两用模式中，通过天线 1102，将加密对话密钥 $[K_s]KP_{media}(2)$ 传递给存储插件 162（步骤 S306）。

在存储插件 160 中，由秘密解密密钥 $K_{media}(1)$ 解密抽出对话密钥 K_s （步骤 S318）。

同样地，在存储插件 162 中也是由秘密解密密钥 $K_{media}(2)$ ，解密抽出对话密钥 K_s （步骤 S320）。

以下处理与图 15 中说明过的实施例 3 的存储插件 140 及 142 的动作相同，因此，其说明不重复。

按照这样的结构，存储插件自身将公开加密密钥 $KP_{media}(1)$ 及 $KP_{media}(2)$ 发送到传送对话密钥 K_s 侧（便携式电话机 100）之后，能够进行移动模式。

另外，关于复制模式，存储插件 160 及 162 的动作与实施例 3 的存储插件 140 及 142 的动作相同。

另外，在以上说明中，作为设有寄存器 1500 的结构进行了说明，但与图 5 所示实施例 1 的存储插件 110 相同，也可以是不设寄存器 1500 的结构。

另外，在以上说明中，来自内容服务器 10 的加密数据解密用的电路是置入可在便携式电话装卸的存储插件内的结构，但例如也可以是设置于便携式电话机内部的结构。更一般的是，可以置入可在访问信息服务器的终端设备上装卸的存储插件内的结构，又可以是事先置入该终端设备的结构。

进而，与图 17 中说明过的实施例 3 变形例的存储插件的动作相同，作为许可 ID 数据 License-ID，结构不仅包含乐曲名的特定信息，而且包含再生次数限制信息，也可以是限制用户能够再生内容数据的次数的结构。

[实施例 6]

图 24 是说明本发明实施例 6 的存储插件 170 结构用的概略框图，是实施例 4 的图 18 的对比图。

与实施例 4 的存储插件 150 结构不同点是，第 1 KP_{media} 保持部

1440 接收保持通过数据总线 BS3 从其它媒体发送的公开加密密钥，如公开加密密钥 KPmedia (2)，加密处理部 1430 是通过该公开加密密钥 KPmedia (2)，将对话密钥 Ks 加密，提供给数据总线 BS3 的结构。

- 5 另外，存储插件 170 的结构包含第 2 KPmedia 保持部 1450，能够保持对应于自身的公开加密密钥 KPmedia (1)，向数据总线 BS3 输出。

其它结构与图 18 所示实施例 4 的存储插件 150 结构相同，因此同一部分附加相同符号，其说明不重复。

- 10 图 25 是说明存储插件 170 移动处理用的流程图，是实施例 4 的图 19 的对比图。

参照图 25，首先，在图 25 中也是，设定便携式电话机 100 为发送侧，便携式电话机 102 为接收侧。另外，便携式电话机 102 中也装有与存储插件 170 相同结构的存储插件 172。

- 15 便携式电话机 100 首先向自身侧的存储插件 170 和插入接收侧便携式电话机 102 的存储插件 172 输出移动请求（步骤 S300）。

- 存储插件 172 通过便携式电话机 102 及 100 将对应于自身的公开加密密钥 KPmedia (2) 从第 2KPmedia 保持部 1450 向存储插件 170 发送（步骤 S301），存储插件 170 接收公开加密密钥 KPmedia (2)，
20 存入第 1 KPmedia 保持部 1440（步骤 S302）。

- 另外，在便携式电话机 100 侧，存储插件 170 内的对话密钥发生电路 1432 生成对话密钥 Ks（步骤 S312），使用公开加密密钥 KPmedia (2)，加密处理部 1430 将对话密钥 Ks 加密（步骤 S314），比如，在收发两用模式中，通过天线 1102 将加密对话密钥 [Ks]Kmedia (2) 向存储插件 172 传递（步骤 S316）。
25

在存储插件 172 中，解密处理部 1404 通过秘密解密密钥 Kmedia (2)，解密抽出对话密钥 Ks（步骤 S320）。

以下动作与图 19 所示存储插件 150 及 152 的动作相同，因此其说明不重复。

- 30 通过采用上述结构，按照存储插件 150 的种类，即使在公开加密密钥 KPmedia 的值不同那样的场合等时，也与实施例 4 的存储插件所起的效果相同，比如，从存储插件 170 向存储插件 172 的数据移动，

不通过有上述那样对话密钥发生电路的便携式电话机,通过可连接存储插件与存储插件的接口设备也能进行,有更加方便用户的效果。

而且,许可 ID 数据 License-ID 等被存入寄存器 1500,控制器 1420 可以参照它,因此,能够减少动作所需处理量。

5 另外,在本实施例中,也可以是限制用户能再生内容数据的次数的结构。

另外,在本实施例中也是,与图 10 所示实施例 2 的存储插件 130 相同,也可以是不设寄存器 1500 的结构。

[实施例 7]

10 实施例 7 的存储插件 180 的特征之一是其结构与实施例 4 的存储插件 150 不同,发布服务器、便携式电话机及存储插件分别生成各自的对话密钥。即发布服务器或便携式电话机产生的对话密钥设为 K_s ,一方的存储插件 180 产生的对话密钥设为 K_{s1} ,与存储插件 180 有同样结构的另一方的存储插件 182 产生的对话密钥设为 K_{s2} 。

15 另外,在再生模式中,便携式电话机侧接收存储插件生成的对话密钥用的公开加密密钥设为 K_{Pp} ,能够将由该公开加密密钥 K_{Pp} 加密的数据解密的秘密解密密钥设为 K_p 。

图 26 是说明实施例 7 中便携式电话机 101 结构用的概略框图。

20 与图 5 所示便携式电话机 100 结构的不同点,首先,装有存储插件 180,除此以外,便携式电话机 101 包含 K_{Pp} 保持部 1524,其保持公开加密密钥 K_{Pp} ,在再生模式时,向数据总线 BS2 输出密钥 K_{Pp} 。

另外,便携式电话机 101 的结构还包含: K_p 保持部 1520,保持秘密解密密钥 K_p ;解密处理部 1522,根据由该 K_p 保持部 1520 提供的密钥 K_p ,解密抽出通过数据总线 BS2 由存储插件 180 提供的密钥 K_{Pp} 加密的对话密钥 K_{s1} 。而且,加密处理部 1504 通过由该解密处理部 1522 提供的对话密钥 K_{s1} ,将来自 K_s 发生部 1502 自身的对话密钥 K_s 加密,向数据总线 BS2 输出。

30 便携式电话机 101 的其它方面结构与图 5 所示实施例 1 的便携式电话机 100 的结构相同,因此,同一部分附加相同符号,其说明不重复。

图 27 是表示对应于实施例 7 存储插件 180 的内容服务器 11 结构的概略框图。与图 3 所示内容服务器 10 结构的不同点是,数据处理

部 310 中的加密处理部 322 不是根据来自 Ks 发生部 314 的对话密钥 Ks, 而是根据从装于便携式电话机的存储插件通过对话密钥 Ks 加密发送、由解密处理部 318 解密抽出的对话密钥如对话密钥 Ks1, 将加密处理部 320 的输出进一步加密, 通过数据总线 BS1, 提供给通信装置 350.

内容服务器 11 的其它方面, 结构与图 3 所示实施例 1 的内容服务器 10 的结构相同, 因此, 同一部分附加相同符号, 其说明不重复.

图 28 是说明本发明实施例 7 的存储插件 180 结构用的概略框图, 是实施例 4 图 18 的对比图.

存储插件 180 的结构与存储插件 150 结构的不同点是, 首先对话密钥 Ks1 发生部 1432 产生该插件独自の对话密钥 Ks1.

存储插件 180 还包含转换开关 1436, 接收在插件这一媒体保持固有公开加密密钥 KPmedia 的 KPmedia 保持部 1440 的输出和通过数据总线 BS3 由便携式电话机 101 提供的公开加密密钥 KPp, 按照动作模式输出某一方. 转换开关 1436 有接点 Pi 及 Ph, 接点 Pi 与数据总线 BS3 结合, 接点 Ph 与 KPmedia 保持部 1440 结合. 加密处理部 1430 通过由转换开关 1436 提供的公开加密密钥 KPmedia 或公开加密密钥 KPp 之一, 将来自 Ks1 发生部 1432 的对话密钥 Ks1 加密, 提供给数据总线 BS3.

即, 转换开关 1436 在发布模式时及移动模式中变为移动终点时是未使用状态; 处于再生模式时, 接点 Pi 侧关闭; 移动模式中变为移动起点时, 接点 Ph 侧关闭.

存储插件 180 还包含转换开关 1435 代替转换开关 1434, 有接点 Pe、Pf 及 Pg, 接收来自解密处理部 1404 提供的内容服务器 11 的对话密钥 Ks、Ks1 发生部 1432 的输出、来自数据总线 BS4 提供的便携式电话机 101 的对话密钥 Ks, 按照动作模式选择性输出某一个. 来自解密处理部 1404 的输出与接点 Pe 结合, Ks1 发生部 1432 的输出与接点 Pf 结合, 数据总线 BS4 与接点 Pg 结合. 因而, 加密处理部 1406 与解密处理部 1410 根据从该转换开关 1435 提供的密钥, 分别进行加密处理及解密处理.

即, 转换开关 1435 在发布模式的场合, 进行来自内容服务器 11 的对话密钥的抽出时, 接点 Pe 侧关闭; 发布模式的场合, 对来自发

布服务器的加密许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 进行由密钥 Ks1 的解密时,接点 Pf 侧关闭.转换开关 1435 在再生模式中进行解密处理时,接点 Pf 侧关闭;在再生模式中进行加密处理时,接点 Pg 侧关闭.转换开关 1435 在移动模式中变为移动起点的场合进行解密处理时,接点 Pf 侧关闭;在移动模式中变为移动起点的场合进行加密处理时,接点 Pg 侧关闭.转换开关 1435 在移动模式中变为移动终点的场合接收移动起点的对话密钥时,接点 Pe 侧关闭;在移动模式中变为移动终点的场合接收许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 时,接点 Pf 侧关闭.

10 存储插件 180 还包含转换开关 1409 代替转换开关 1408,有接点 Pa、Pb、Pc、Pe,接收从 Ks1 发生部 1432 提供的自身对话密钥 Ks1; KPcard 保持部 1405 的输出;由数据总线 BS5 提供的许可密钥 Kc;接收由加密处理部 1414 提供、由对方的公开加密密钥 KPcard(n)加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID,按照动作模式选择性输出之一.来自 Ks1 发生部 1432 的输出与接点 Pa 结合, KPcard 保持部 1405 的输出与接点 Pb 结合,数据总线 BS5 与接点 Pc 结合,加密处理部 1414 的输出与接点 Pd 结合.因而,加密处理部 1406 对从该转换开关 1409 提供的数据分别进行加密处理.

即,转换开关 1409 在发布模式中变为发布对象的场合,向内容服务器 11 发送自身公开加密密钥 KPcard(1)或自身对话密钥 Ks1 时,依次接点 Pb 侧及接点 Pa 侧关闭.转换开关 1409 在再生模式时,接点 Pc 侧关闭;在移动模式中变为移动起点时,接点 Pd 侧关闭.转换开关 1409 在移动模式中变为移动终点的场合,向移动起点发送自身公开加密密钥 KPcard(1)或自身对话密钥 Ks1 时,依次接点 Pb 侧及接点 Pa 侧关闭.

图 29 是说明使用图 28 说明过的存储插件 180 的发布模式用的流程图.

在图 28 中,说明了用户 1 使用存储插件 180 从内容服务器 11 接收内容数据发布时的动作.

30 首先,从用户 1 的便携式电话机 101 通过用户触摸键 1108 的操作等,向内容服务器 11 发送发布请求(步骤 S100).

在内容服务器 11 中,按照该发布请求,对话密钥发生部 314 生

成对话密钥 K_s (步骤 S103)。另一方面, 在存储插件 180 侧, K_{s1} 发生部 1432 生成对话密钥 K_{s1} (步骤 S103')。

在内容服务器 11 中, 接着, 内容服务器 11 内的加密处理部 316 通过公开加密密钥 KP_{media} , 将对话密钥 K_s 进行加密处理, 提供给
5 数据总线 $BS1$ (步骤 S104)。

通信装置 350 将来自加密处理部 316 的加密对话密钥 $[K_s]K_{media}$, 通过通信网向便携式电话机 101 的存储插件 180 发送 (步骤 S106)。

在存储插件 180 中, 解密处理部 1404 将通过存储器接口 1200 提
10 供给数据总线 $BS3$ 的接收数据, 通过由秘密解密密钥 K_{media} 进行解密处理, 将对话密钥 K_s 解密抽出 (步骤 S108)。

接着, 在发布模式中, 首先, 转换开关 1409 选择接点 P_b 关闭的状态, 因此, 加密处理部 1406 通过接点 P_b , 接收从 $KP_{card}(1)$ 保持部 1405 提供的公开加密密钥 $KP_{card}(1)$ (用户 1 的存储插件中的公开加密密钥), 接着, 转换开关 1409 变为接点 P_a 关闭的状态,
15 加密处理部 1406 通过接点 P_a 接收从 K_{s1} 保持部 1432 提供的对话密钥 K_{s1} 。转换开关 1435 选择接点 P_e 关闭的状态, 因此, 加密处理部 1406 通过来自解密处理部 1404 的对话密钥 K_s , 将公开加密密钥 $KP_{card}(1)$ 及对话密钥 K_{s1} 加密, 提供给数据总线 $BS3$ 。

20 便携式电话机 101 将由加密处理部 1406 加密的数据 $[KP_{card}(1), K_{s1}] K_s$, 向内容服务器 11 输出 (步骤 S112)。

在服务器 31 中, 解密处理部 318 将由通信装置 350 接收、提供给数据总线 $BS1$ 的数据 $[KP_{card}(1), K_{s1}] K_s$, 通过对话密钥 K_s 进行解密处理, 解密抽出公开加密密钥 $KP_{card}(1)$ 及对话密钥 K_{s1}
25 (步骤 S114)。

接着, 发布控制部 312 从发布信息数据库 304 取得许可密钥 K_c (步骤 S116) 且以保持于发布信息数据库 304 等的数据为基础, 生成许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据 (步骤 S118)。

30 加密处理部 320 接收来自发布控制部 312 的许可密钥 K_c 、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据, 通过由解密处理部 318 提供的公开加密密钥 $KP_{card}(1)$ 进行加密处理 (步骤 S120)。

加密处理部 322 接收由加密处理部 320 加密的数据,再由对话密钥 Ks1 加密,提供给数据总线 BS1 (步骤 S122)。

通信装置 350 向插件 180 发送由加密处理部 322 加密的数据 $[[Kc, License-ID, User-ID] Kcard(1)]Ks1$ 。

- 5 在插件 180 中,转换开关 1435 被转换为选择接点 Pf 关闭状态,因此,解密处理部 1410 通过来自 Ks1 发生部 1432 的对话密钥 Ks1 进行解密处理,抽出数据 $[Kc, License-ID, User-ID]Kcard(1)$ (步骤 S126), 存入存储器 1412 (步骤 S128)。

- 10 进而,在存储插件 180 中,解密处理部 1416 将存入存储器 1412 的数据 $[Kc, License-ID, User-ID]Kcard(1)$ 解密,控制器 1420 将解密的数据 License-ID、User-ID 存入寄存器 1500 (步骤 129)。

另一方面,内容服务器 11 从发布信息数据库 304 取得加密内容数据 $[Dc]Kc$,通过通信装置 350,向存储插件 180 发送(步骤 S130)。

- 15 在存储插件 180 中,将接收的加密内容数据 $[Dc]Kc$ 直接存入存储器 1412 (步骤 S132)。

通过以上动作,存储插件 180 变为内容数据可再生状态。

图 30 是说明在便携式电话机 101 内,从保持于实施例 7 的存储插件 180 的加密内容数据,将内容数据解密,作为音乐向外部输出用再生模式的流程图。

- 20 参照图 30,根据来自便携式电话机触摸键 1108 等的用户 1 的指示,向存储插件 180 输出再生请求(步骤 S200)。

在存储插件 180 中,控制器 1420 从寄存器 1500 读出许可 ID 数据 License-ID、用户 ID 数据 User-ID 等(步骤 S205)。

- 25 控制器 1420 根据解密许可 ID 数据 License-ID 等所含信息,判断由许可 ID 数据 License-ID 中的数据指定的内容数据(音乐数据)再生处理累计数是否超过可以再生次数的上限值(步骤 S206),判断为没有超过可以再生次数的场合,向便携式电话机 101 的控制器 1106 发送再生许可通知(步骤 S208)。

- 30 在便携式电话机 101 中,首先向存储插件 180 发送公开加密密钥 KPp,对话密钥发生电路 1502 生成对话密钥 Ks (步骤 S210)。

另一方面,也由存储插件 180 生成对话密钥 Ks1 (步骤 S210'),由公开加密密钥 KPp 将对话密钥 Ks1 加密(步骤 S211),向便携式

电话机 101 发送加密对话密钥 $[Ks1]Kp$ (步骤 S212)。

在便携式电话机 101 中,解密处理部 1522 通过秘密解密密钥 Kp , 将通过数据总线 BS2 由存储插件 180 提供的加密对话密钥 $[Ks1]Kp$ 解密, 抽出对话密钥 $Ks1$ (步骤 S213), 加密处理部 1504 通过对话密
5 钥 $Ks1$ 将对话密钥 Ks 加密 (步骤 S214), 向数据总线 BS2 输出加密对话密钥 $[Ks]Ks1$ (步骤 S215)。

存储插件 180 通过数据总线 BS3, 接收由便携式电话机 101 生成的加密对话密钥 $[Ks]Ks1$, 由对话密钥 $Ks1$ 解密, 抽出对话密钥 Ks (步骤 S216)。

10 进一步, 存储插件 180 按照进行再生处理, 更新寄存器 1500 中许可 ID 数据 License-ID 中的再生处理累计数方面的数据 (步骤 217)。

接着, 存储插件 180 从存储器 1412 读出加密的数据 $[Kc, License-ID, User-ID]Kcard(1)$, 解密处理部 1416 进行解密, 抽
15 出许可密钥 Kc (步骤 S218)。

接着, 通过抽出的对话密钥 Ks 将许可密钥 Kc 加密 (步骤 S219), 将加密许可密钥 $[Kc]Ks$ 提供给数据总线 BS2 (步骤 S220)。

便携式电话机 101 的解密处理部 1506 通过由对话密钥 Ks 进行解密处理, 取得许可密钥 Kc (步骤 S222)。

20 接着, 存储插件 180 将加密内容数据 $[Dc]Kc$ 从存储器 1412 读出, 提供给数据总线 BS2 (步骤 S224)。

便携式电话机音乐再生部 1508 将加密内容数据 $[Dc]Kc$ 由抽出的许可密钥 Kc 进行解密处理 (步骤 S226), 再生内容数据, 提供给混合部 1510 (步骤 S228)。

25 另一方面, 在步骤 S206 中, 判断为控制器 1420 不能进行解密处理的场合, 存储插件 180 向便携式电话机 101 发送再生不许可通知 (步骤 S230)。

按照上述结构, 存储插件及便携式电话机即使生成独自の对话密钥的场合, 也能够限制用户可再生内容数据的次数。

30 图 31 是说明在实施例 7 的 2 个存储插件间, 进行内容数据及密钥数据等移动处理用的流程图。

参照图 31, 首先, 在图 31 中, 设定便携式电话机 101 为发送侧,

与其结构相同的便携式电话机 103 为接收侧。另外，便携式电话机 103 也装有与存储插件 180 结构相同的存储插件 182。

便携式电话机 101 首先向自身侧的存储插件 180 和插入接收侧便携式电话机 103 的存储插件 182 输出移动请求（步骤 S300）。

- 5 由此，在便携式电话机 101 中，存储插件 180 内的对话密钥发生电路 1432 生成对话密钥 Ks1（步骤 S312），另一方面，在便携式电话机 103 中，存储插件 182 内的对话密钥发生电路 1432 生成对话密钥 Ks2（步骤 S312'）。

- 10 在便携式电话机 101 中，存储插件 180 使用公开加密密钥 Kpmedia，加密处理部 1430 将对话密钥 Ks1 加密（步骤 S314），比如，在收发两用模式中，通过天线 1102，将加密对话密钥 [Ks]Kmedia 传递给存储插件 182（步骤 S316）。

- 15 在存储插件 182 中，解密处理部 1404 通过秘密解密密钥 Kmedia 解密抽出对话密钥 Ks1（步骤 S320），再由对话密钥 Ks1 将存储插件 182 的公开加密密钥 KPcard(2) 及对话密钥 Ks2 加密（步骤 S322），向存储插件 180 发送加密的数据 [KPcard(2), Ks2]Ks1（步骤 S324）。

- 20 在存储插件 180 中，解密处理部 1410 通过对话密钥 Ks1 将从存储插件 182 发送的加密数据解密，将存储插件 182 的公开加密密钥 KPcard(2) 及对话密钥 Ks2 解密抽出（步骤 S326）。这时，在转换开关 1435，接点 Pf 关闭，来自 Ks1 发生电路 1432 的密钥 Ks1 被提供给解密处理部 1410。

接着，在存储插件 180 中，从存储器 1412 读出由存储插件 150 的公开加密密钥 Kcard(1) 加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID（步骤 S328）。

- 25 接着，解密处理部 1416 通过秘密解密密钥 Kcard(1)，将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 进行解密处理（步骤 S330）。

- 30 控制器 1420 将这样被解密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 的值与寄存器 1500 内的数据值置换（步骤 S331）。

进一步，加密处理部 1414 通过在解密处理部 1410 抽出的插件 182 中的公开加密密钥 KPcard(2)，将许可密钥 Kc、许可 ID 数据

License-ID、用户 ID 数据 User-ID 加密（步骤 S332）。

由加密处理部 1414 加密的数据，通过转换开关 1409（接点 Pd 关闭），再被提供给加密处理部 1406，加密处理部 1406 通过存储插件 182 的对话密钥 Ks2，将数据[Kc, License-ID, User-ID]Kcard
5 （2）加密（步骤 S334）。这时，转换开关 1435 接点 Pg 关闭，来自解密处理电路 1410 的对话密钥 Ks2 被提供给加密处理部 1406。

接着，存储插件 180 通过便携式电话机 101，向存储插件 152 发送加密的数据[[Kc, License-ID, User-ID]Kcard（2）]Ks2（步骤 S336）。

10 在存储插件 182 中，将从存储插件 180 发送的数据，由解密处理部 1410，根据对话密钥 Ks2，进行解密处理，存入存储器 1412（步骤 S339）。进而，存储插件 182 根据许可密钥 Kcard（2），将数据[Kc, License-ID, User-ID]Kcard（2）解密，将解密的许可 ID 数据 License-ID、用户 ID 数据 User-ID 存入寄存器 1500（步骤 S341）。

15 另一方面，存储插件 180 再将存入寄存器 1500 的许可 ID 数据 License-ID 及用户 ID 数据 User-ID 清除（步骤 S343）。

接着，存储插件 180 将加密内容数据[Dc]Kc 从存储器读出，向存储插件 182 发送（步骤 S344）。

20 存储插件 182 将接收的加密内容数据，直接存入存储器 1412（步骤 S346）。

当进行上述处理，在步骤 S342 中，许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等被从存储插件 180 中清除，因此，存储插件 180 变为“状态 SB”。

25 另一方面，在存储插件 182 中，除加密内容数据以外，许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等所有数据也被移动，因此，存储插件 182 变为“状态 SA”。

由于采用上述结构，比如，不通过有上述那样的对话密钥发生电路 1502 的便携式电话机，通过可连接存储插件与存储插件的接口设备，也能进行从存储插件 180 向存储插件 182 的数据移动，有更加方便用户的效果。
30

而且，许可 ID 数据 License-ID 等被存入寄存器 1500，控制器 1420 可以参照它，因此，能够减少动作所需处理量。

另外，在各便携式电话机、存储插件的对话密钥都各不相同，因此，进一步提高了通信的安全性。

在这里，移动时，关于限制再生信息内再生次数的许可 ID 数据 License-ID，将记录于存储器 1412 的许可 ID 数据 License-ID 变更为记录了由寄存器 1500 每次再生被修正的再生次数的许可 ID 数据 License-ID，构成新的再生信息。这样，即使内容数据在存储插件间移动，再生次数有限制的内容数据的再生次数也不会超过发布时确定的再生次数的限制。

[实施例 8]

10 实施例 8 的便携式电话机 105 及存储插件 190，如以下说明，其特征是与实施例 7 的便携式电话机 101 及存储插件 180 的结构有以下不同点。

即，在实施例 8 的便携式电话机 105 中含有，比如，预先在发布系统中的认证机构等管理部门登记该便携式电话机 105 时，将分配于该便携式电话机 105 的公开加密密钥 KPp 及认证数据 Crtf，以由公开解密密钥（公开认证密钥）KPmaster 加密的形式记录保持的单元。

同样，在实施例 8 的存储插件 190 中也含有，比如，预先在发布系统中的认证机构等管理部分登记该存储插件 190 时，将分配于该存储插件的公开加密密钥 KPmedia 及认证数据 Crtf，以由公开解密密钥（公开认证密钥）KPmaster 加密的形式记录保持的单元。

在这里，存储插件 190 及实施例 8 的内容服务器 12 中含有记录保持该公开解密密钥（公开认证密钥）KPmaster 的单元。该公开解密密钥（公开认证密钥）KPmaster 是系统通用密钥，用于证明系统中进行数据输出的所有设备是在与对话密钥交换方面能够相互进行数据授受的设备，以及用于获得向对方传送对话密钥时使用的密码密钥。

以下进一步详细说明实施例 8 的便携式电话机 105、存储插件 190 及内容服务器 12 的结构。

图 32 是说明实施例 8 中便携式电话机 105 结构用的概略框图。

30 与图 26 所示便携式电话机 101 结构的不同点是，代替 KPp 保持部 1524，包含 [KPp, Crtf]KPmaster 保持部 1525，用于保持由公开解密密钥（公开认证密钥）KPmaster 加密的公开密码密钥 KPp 及认

证数据 Crtf.

便携式电话机 105 的其它方面, 结构与图 26 所示实施例 7 的便携式电话机 101 的结构相同, 因此, 同一部分附加相同符号, 其说明不重复。

5 图 33 是表示对应于实施例 8 的存储插件 190 的内容服务器 12 结构的概略框图。与图 27 所示内容服务器 11 结构的不同点是, 数据处理部 310 还包含: KPmaster 保持部 324, 保持公开解密密钥 KPmaster; 解密处理部 326, 用于根据从 KPmaster 保持部 324 输出的公开解密密钥 KPmaster, 将通过通信装置 350 从通信网提供给数据总线 BS1 的数据解密。加密处理部 316 通过由在解密处理部 326 的解密处理抽出的公开加密密钥 KPmedia, 将在 Ks 发生部 314 产生的对话密钥 Ks 加密, 另外, 发布控制部 312 通过由在解密处理部 326 的解密处理抽出的认证数据 Crtf, 认证请求发布的存储插件是否是正式的存储插件。

15 内容服务器 12 的其它方面结构与图 27 所示实施例 7 的内容服务器 11 的结构相同, 所以, 同一部分附加相同符号, 其说明不重复。

图 34 是说明本发明实施例 8 的存储插件 190 结构用的概略框图, 是实施例 7 的图 28 的对比图。

实施例 8 的存储插件 190 的结构与实施例 7 的存储插件 180 结构的不同点是, 首先, 存储插件 190 结构包含 [KPmedia, Crtf] KPmaster 保持部 1442, 以由公开解密密钥 (公开认证密钥) KPmaster 加密的形式记录保持公开密码密钥 KPmedia 及证明数据 Crtf。另一方面, 转换开关 1436 被省略, [KPmedia, Crtf] KPmaster 保持部 1442 的输出被直接提供给数据总线 BS3。

25 存储插件 190 还包含: KPmaster 保持部 1450, 用于记录保持公开解密密钥 KPmaster; 解密处理部 1452, 用于根据从 KPmaster 保持部 1450 输出的公开解密密钥 KPmaster, 将数据总线 BS3 上的数据解密。

在通过解密处理部 1452 的解密处理抽出的公开加密密钥 KPmedia 及认证数据 Crtf 中的公开加密密钥 KPmedia 被提供给加密处理部 1430, 认证数据 Crtf 通过数据总线 BS5 被提供给控制器 1420。

存储插件 190 的其它结构与图 28 所示存储插件 180 结构相同，因此，同一部分附加相同符号，其说明不重复。

图 35 是表示图 34 所示存储插件 190 内记录空间结构的概略框图。包含：安全区域 1490，存储插件独自管理、用户不能自由改写
5 读出其内容，且由对不当开封处理，破坏内部数据的 TRM 模块构成；准安全区域 1491，虽然用户能够确认数据存在，但是，该数据存储插件固有的加密，在这里，由公开加密密钥 KPcard (1) 施行加密并记录，不能自由改写数据；非安全区域 1492，用户能够自由读出、改写其内容。

10 安全区域 1490 设有：存储插件 190 出厂时保持的密钥保持部，即 Kmedia 保持部 1402、KPcard (1) 保持部 1405、Kcard (1) 保持部 1415、[KPmedia, Crtf]KPmaster 保持部 1442、KPmaster 保持部 1450 和被存入明码电文许可信息的寄存器 1500。

在准安全区域 1491 存入将存储插件 1900 固有的加密数据 [Kc, License-ID, User-ID]Kcard (1)，设于存储器 1412 内。

在非安全区域 1493 存入加密内容数据 [Dc]Kc，设于存储器 1412 内。因而，成为加密内容数据 [Dc]Kc 能够自由复制、但不能复制再生所需数据的结构。因为即使将存入准安全区域 1491 的许可信息复制于其它存储插件，也不能由没有对的秘密解密密钥 Kcard (1) 的
20 其它保密插件，复制由存储插件 1900 固有的公开密码密钥 KPcard (1) 进行的加密。

另外，虽然说明了将保持密钥的所有密钥保持部设置于安全区域，但是，可以只将保持秘密解密密钥的 Kmedia 保持部 1402 及 Kcard (1) 保持部 1415 配置于安全区域，其它密钥保持部保持的密钥可以
25 配置于可从外部参照的 ROM (Read Only Memory)。

图 36 是说明使用图 35 说明过的存储插件 190 的发布模式用的流程图。

在图 36 中，说明了用户 1 通过使用存储插件 190，从内容服务器 12 接收内容数据发布时的动作。

30 首先，从用户 1 的便携式电话机 105 通过用户的触摸键 1108 的操作等，向存储插件 190 进行发布请求（步骤 S400）。

从存储插件 190，由 [KPmedia, Crtf]KPmaster 保持部 1442，经

由便携式电话机 105, 向内容服务器 12 发送加密数据 [KPmedia, Crtf]KPmaster (步骤 S402)。

在内容服务器 12 中, 当接收加密数据 [KPmedia, Crtf]KPmaster, 根据 KPmaster 保持部 324 保持的公开解密密钥 KPmaster, 通过解密处理部 326 解密处理, 取得公开加密密钥 KPmedia 及认证数据 Crtf (步骤 S404)。

进一步, 在内容服务器 12 中, 根据认证数据 Crtf 进行存储插件 190 的认证 (步骤 S406), 如果证明存储插件 190 是正式的存储插件, 进行转移到 S412 的处理。另一方面, 在不被证明存储插件 190 是正式存储插件的场合, 内容服务器 12 发送发布不许可通知 (步骤 S408), 便携式电话机 105 接收发布不许可通知 (步骤 S410)。

在证明存储插件 190 是正式存储插件的场合, 在内容服务器 12, 对话密钥发生部 314 生成对话密钥 Ks (步骤 S412)。

在内容服务器 12 中, 接着, 内容服务器 12 内的加密处理部 316 通过公开加密密钥 KPmedia, 将对话密钥 Ks 进行加密处理, 提供给数据总线 BS1 (步骤 S414)。

通信装置 350 将来自加密处理部 316 的加密对话密钥 [Ks]Kmedia, 通过通信网, 向便携式电话机 105 的存储插件 190 发送 (步骤 S416)。

在存储插件 190 中, 解密处理部 1404 将通过存储器接口 1200 提供给数据总线 BS3 的接收数据, 通过由秘密解密密钥 Kmedia 进行解密处理, 解密抽出对话密钥 Ks (步骤 S418)。进而, 在存储插件 190 中, Ks1 发生部 1432 生成对话密钥 Ks1 (步骤 S420)。

接着, 在发布模式中, 首先, 转换开关 1409 选择接点 Pb 关闭的状态, 因此, 加密处理部 1406 通过接点 Pb, 接收从 KPcard (1) 保持部 1405 提供的公开加密密钥 KPcard (1), 接着, 转换开关 1409 变为接点 Pa 关闭状态, 加密处理部 1406 通过接点 Pa 接收从 Ks1 发生部 1432 提供的对话密钥 Ks1。因为转换开关 1435 选择接点 Pe 关闭的状态, 所以加密处理部 1406 通过来自解密处理部 1404 的对话密钥 Ks, 将公开加密密钥 KPcard (1) 及对话密钥 Ks1 加密, 提供给数据总线 BS3 (步骤 S422)。

通过便携式电话机 105 向内容服务器 12 发送由加密处理部 1406

加密的数据[KPcard(1), Ks1]Ks(步骤 S424)。

在内容服务器 12 中, 解密处理部 318 将由通信装置 350 接收、
提供给数据总线 BS1 的数据[KPcard(1), Ks1] Ks, 通过对话密钥
Ks 进行解密处理, 解密抽出公开加密密钥 KPcard(1) 及对话密钥
5 Ks1(步骤 S426)。

接着, 发布控制部 312 从发布信息数据库 304 取得许可密钥 Kc
(步骤 S428), 且以发布信息数据库 304 等保持的数据为基础, 生
成许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据(步骤
S430)。

10 加密处理部 320 接收来自发布控制部 312 的许可密钥 Kc、许可
ID 数据 License-ID 及用户 ID 数据 User-ID 等数据, 通过由解密处
理部 318 提供的公开加密密钥 KPcard(1)进行加密处理(步骤 S432)。

加密处理部 322 接收由加密处理部 320 加密的数据, 再由对话密
钥 Ks1 加密, 提供给数据总线 BS1(步骤 S434)。

15 通信装置 350 将由加密处理部 322 加密的数据[[Kc, License-
ID, User-ID]Kcard(1)]Ks1, 向存储插件 190 发送(步骤 S436)。

在存储插件 190 中, 转换开关 1435 被转换为选择接点 Pf 呈关闭
状态的状态, 因此, 解密处理部 1410 通过来自 Ks1 发生部 1432 的对
话密钥 Ks1, 进行解密处理, 抽出数据[Kc, License-ID, User-
20 ID]Kcard(1)(步骤 S438)、存入存储器 1412(步骤 S440)。

进一步, 在存储插件 190 中, 解密处理部 1416 将存入存储器 1412
的数据[Kc, License-ID, User-ID]Kcard(1)解密, 控制器 1420
将被解密的数据 License-ID、User-ID 存入寄存器 1500(步骤 442)。

另一方面, 内容服务器 12 从发布信息数据库 304 取得加密内容
25 数据[Dc]Kc, 通过通信装置 350 向存储插件 180 发送(步骤 S444)。

在存储插件 190 中, 将接收的加密内容数据[Dc]Kc 直接存入存
储器 1412(步骤 S446)。

通过上述动作, 存储插件 190 变为内容数据可再生状态。

图 37 是说明在便携式电话机 105 内, 从保持于实施例 8 的存储
30 插件 190 的加密内容数据, 将内容数据解密, 作为音乐向外部输出用
的再生模式的流程图。

参照图 37, 根据来自便携式电话机的密钥盘 1108 等的用户 1 的

指示, 向便携式电话机 105 提供再生请求时 (步骤 S500), 从便携式电话机 105 向存储插件 190 发送加密数据 [KPp, Crtf] KPmaster (步骤 S502)。

在存储插件 190 中, 通过由解密处理部 1452 中的公开解密密钥 KPmaster 的解密处理, 取得公开加密密钥 KPp 及认证数据 Crtf (步骤 S504)。控制器 1420 根据认证数据 Crtf, 认证便携式电话机 105 是否是正式设备 (步骤 S506), 当证明是正式设备时, 处理转移到步骤 S508, 当不被证明是正式设备时, 将再生不许可通知向便携式电话机 105 发送 (步骤 S544)。

证明便携式电话机 105 是正式设备的场合 (步骤 S506), 对话密钥发生部 1432 生成对话密钥 Ks1 (步骤 S508)。加密处理部 1430 根据来自解密处理部 1452 的公开加密密钥 KPp, 将对话密钥 Ks1 加密 (步骤 S510), 从存储插件 190 向便携式电话机 105 发送加密对话密钥 [Ks1] Kp (步骤 S512)。

在便携式电话机 105 中, 通过在解密处理部 1522 的解密处理, 对话密钥 Ks1 被解密抽出 (步骤 S514)。接着, 在对话密钥发生部 1502 中, 生成对话密钥 Ks (步骤 S516), 加密处理部 1504 通过对对话密钥 Ks1 将密钥 Ks 加密 (步骤 S518), 从便携式电话机 105 向存储插件 190 发送加密对话密钥 [Ks] Ks1 (步骤 S520)。

在存储插件 190 中, 解密处理部 1410 通过对对话密钥 Ks1, 将加密对话密钥 [Ks] Ks1 解密处理, 抽出对话密钥 Ks (步骤 S522)。进而, 在存储插件 190 中, 控制器 1420 从寄存器 1500 读出许可 ID 数据 License-ID、用户 ID 数据 User-ID 等 (步骤 S524)。

控制器 1420 根据含于被解密的许可 ID 数据 License-ID 等的信息, 判断由许可 ID 数据 License-ID 中的数据指定的内容数据 (音乐数据) 再生处理的累计数是否超过可以再生次数的上限值 (步骤 S526), 判断为超过可以再生次数的场合, 存储插件 190 按照进行再生处理, 更新寄存器 1500 中许可 ID 数据 License-ID 内的再生处理累计数方面的数据 (步骤 528)。

接着, 存储插件 190 从存储器 1412 读出被加密的数据 [Kc, License-ID, User-ID] Kcard (1), 解密处理部 1416 进行解密, 抽出许可密钥 Kc (步骤 S530)。

接着，通过在步骤 S522 抽出的对话密钥 K_s ，将许可密钥 K_c 加密（步骤 S532），将加密许可密钥 $[K_c] K_s$ 提供给数据总线 BS2（步骤 S534）。

5 便携式电话机 105 的解密处理部 1506 通过由对话密钥 K_s 进行解密处理，取得许可密钥 K_c （步骤 S536）。

接着，存储插件 190 将加密内容数据 $[D_c] K_c$ 从存储器 1412 读出，提供给数据总线 BS2（步骤 S538）。

10 便携式电话机的音乐再生部 1508 将加密内容数据 $[D_c] K_c$ ，通过抽出的许可密钥 K_c 进行解密处理（步骤 S540），再生内容数据，提供给混合部 1510（步骤 S542）。

另一方面，在步骤 S526 中，判断为控制器 1420 解密处理不可能的场合，存储插件 190 向便携式电话机 105 发送再生不许可通知（步骤 S544）。

15 按照上述结构，存储插件及便携式电话机即使生成独自の对话密钥的场合，也能够限制用户可再生内容数据的次数。

图 38 是说明在实施例 8 的 2 个存储插件间，内容数据及密钥数据等移动处理用的流程图。

20 参照图 38，首先，在图 38 中，设定便携式电话机 105 为发送侧，与其结构相同的便携式电话机 107 为接收侧。另外，便携式电话机 107 也装有与存储插件 190 结构相同的存储插件 192。

便携式电话机 105，首先，向插入接收侧便携式电话机 107 的存储插件 192 输出移动请求（步骤 S600）。

由此，从装于便携式电话机 107 的存储插件 192，向存储插件 190 发送加密数据 $[KPmedia, Crtf] KPmaster$ （步骤 S602）。

25 在存储插件 190 中，当接收加密数据 $[KPmedia, Crtf] KPmaster$ 时，根据 $KPmaster$ 保持部 1450 保持的公开解密密钥 $KPmaster$ ，通过解密处理部 1452 解密处理，取得公开加密密钥 $KPmedia$ 及认证数据 $Crtf$ （步骤 S604）。

30 进一步，在存储插件 190 中，根据认证数据 $Crtf$ 进行存储插件 192 的认证（步骤 S606），如果证明存储插件 192 是正式的存储插件，处理转移到 S612。另一方面，如果不被证明存储插件 192 是正式的存储插件的场合，存储插件 190 发送移动不许可通知（步骤 S608），

便携式电话机 107 接收移动不许可通知（步骤 S610）。

证明存储插件 192 是正式存储插件的场合，在存储插件 190 中，对话密钥发生部 1432 生成对话密钥 Ks1（步骤 S612）。

在存储插件 190 中，接着，加密处理部 1430 通过公开加密密钥 KPmedia，将对话密钥 Ks1 进行加密处理，提供给数据总线 BS3（步骤 S614）。

从存储插件 190，将来自加密处理部 1430 的加密对话密钥 [Ks] Kmedia，通过便携式电话机 105，向便携式电话机 107 的存储插件 192 发送（步骤 S616）。

在存储插件 192 中，解密处理部 1404 将通过存储器接口 1200 提供给数据总线 BS3 的接收数据，通过由秘密解密密钥 Kmedia 进行解密处理，解密抽出对话密钥 Ks（步骤 S618）。进而，在存储卡 192 中，与 Ks1 发生器 1432 结构相同的 Ks2 发生部 1432' 生成对话密钥 Ks2（步骤 S620）。

接着，在存储插件 192 中，首先转换开关 1409 选择接点 Pb 关闭的状态，因此，加密处理部 1406 通过接点 Pb 接收由 KPcard(1) 保持部 1405 提供的公开加密密钥 KPcard(1)，接着，转换开关 1409 变为接点 Pa 呈关闭状态，加密处理部 1406 通过接点 Pa 接收从 Ks2 发生部 1432' 提供的对话密钥 Ks2。因为转换开关 1435 选择接点 Pe 关闭的状态，因此，加密处理部 1406 通过来自解密处理部 1404 的对话密钥 Ks1，将公开加密密钥 KPcard(1) 及对话密钥 Ks2 加密，提供给数据总线 BS3（步骤 S622）。

通过便携式电话机 107，向存储插件 190 发送由加密处理部 1406 加密的数据 [KPcard(1)、Ks2] Ks1（步骤 S624）。

在存储插件 190 中，解密处理部 1410 通过对话密钥 Ks1 将从存储插件 192 发送的加密数据解密，解密抽出存储插件 192 的公开加密密钥 KPcard(2) 及对话密钥 Ks2（步骤 S626）。这时，在转换开关 1435，接点 Pf 关闭，来自 Ks1 发生电路 1432 的密钥 Ks1 被提供给解密处理部 1410。

接着，在存储插件 190 中，从存储器 1412 读出由存储插件 190 的公开加密密钥 Kcard(1) 加密的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID（步骤 S628）。

接着, 在存储插件 190 中, 解密处理部 1416 通过秘密解密密钥 Kcard(1), 将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 进行解密处理(步骤 S630)。

存储插件 190 的控制器 1420 将这样被解密的许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 的值与寄存器 1500 内的数据值置换(步骤 S632)。

进一步, 存储插件 190 的加密处理部 1414 通过在解密处理部 1410 抽出的存储插件 192 中的公开加密密钥 KPcard(2), 将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 加密(步骤 S634)。

由存储插件 190 的加密处理部 1414 加密的数据通过转换开关 1409(接点 Pd 关闭), 再被提供给加密处理部 1406, 加密处理部 1406 将数据[Kc, License-ID, User-ID]Kcard(2)通过存储插件 192 的对话密钥 Ks2 加密(步骤 S636)。这时, 转换开关 1435 接点 Pg 关闭, 来自解密处理电路 1410 的对话密钥 Ks2 被提供给加密处理部 1406。

接着, 存储插件 190 通过便携式电话机 105, 向存储插件 192 发送加密的数据[[Kc, License-ID, User-ID]Kcard(2)]Ks2(步骤 S638)。

在存储插件 192 中, 将从存储插件 190 发送的数据, 通过解密处理部 1410, 根据对话密钥 Ks2 进行解密处理, 存入存储器 1412(步骤 S640)。进而, 存储插件 192 根据许可密钥 Kcard(2), 将数据[Kc, License-ID, User-ID]Kcard(2)解密, 将解密的许可 ID 数据 License-ID、用户 ID 数据 User-ID 存入寄存器 1500(步骤 S642)。

另一方面, 存储插件 190 再将存入寄存器 1500 的许可 ID 数据 License-ID 及用户 ID 数据 User-ID 清除(步骤 S644)。

接着, 存储插件 190 将加密内容数据[Dc]Kc 从存储器 1412 读出, 向存储插件 192 发送(步骤 S646)。

存储插件 192 将接收的加密内容数据直接存入存储器 1412(步骤 S648)。

一进行上述处理, 在步骤 S644 中, 许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等就被从存储插件 190 清除, 因此, 存储插件 190 变成“状态 SB”。

另一方面，在存储插件 192 中，除密内容数据以外，许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 等所有数据被移动，因此，存储插件 192 变为“状态 SA”。

在这里，与实施例 7 相同，许可 ID 数据 License-ID 等被存入寄存器 1500，控制器 1420 可以参照它，因此，能够减少动作所需处理量。

另外，对话密钥因便携式电话机、存储插件的不同而不同，因此，更加提高了通信的安全性。

在这里，移动时，关于限制再生信息内再生次数的许可 ID 数据 License-ID，将记录于存储器 1412 中的许可 ID 数据 License-ID 变更为记录了在寄存器 1500 每次再生被修正的再生次数的许可 ID 数据 License-ID，构成新的再生信息。这样，内容数据即使在存储插件间移动，再生次数有限制的内容数据的再生次数也不会超过发布时规定的再生次数的限制。

15 [实施例 9]

图 39 是表示实施例 9 的存储插件 200 结构的概略框图。

实施例 9 的存储插件 200，如以下说明，其特征是与实施例 8 的存储插件 190 的结构有以下不同点。

即，实施例 9 的存储插件 200 的结构为：实施例 8 的存储插件 190 结构中的 Kmedia 保持部 1402、KPCard(1) 保持部 1405、Kcard(1) 保持部 1415、[KPmedia, Crtf]KPmaster 保持部 1442、KPmaster 保持部 1450 及寄存器 1500 被设置于存储器 1412 的规定区域内。由此，转换开关 1409 的接点 Pb 及 Pc 被省略，数据总线 BS4 与存储器 1412 不直接进行数据交换，存储器 1412 只在与数据总线 BS3 之间授受数据。数据总线 BS4 通过数据总线 BS3，与存储器 1412 进行数据授受。

图 40 是表示图 39 所示存储插件 200 内记录空间结构的示意概略图。包含：安全区域 1490，存储插件独自管理，用户不能自由改写读出其内容，且由对于不当开封处理，会破坏内部数据的 TRM 模块构成；非安全区域 1942，用户能够自由读出改写其内容。

在安全区域 1490 中设有从存储插件 200 出厂时保持的密钥保持部，即 Kmedia 保持部 1402、KPCard(1) 保持部 1405、Kcard(1) 保持部 1415、[KPmedia, Crtf]KPmaster 保持部 1442、KPmaster

保持部 1450 和存入明码电文许可信息的寄存器 1500。与实施例 8 中的图 35 的不同点是没有设置准安全区域，为此，将准安全区域 1491 存入的 [Kc, License-ID, User-ID]Kcard (1)，存入由 Kcard (1) 解密的明码电文的许可密钥 Kc、许可 ID License-ID、用户 ID User-ID 内，在实施例 8 中没有存入寄存器 1500 的内容密钥 Kc 也被以明码电文存入安全区域 1490。为此，与实施例 8 相比，安全区域 1490 需要更大的记录空间。

非安全区域 1493 中存入加密内容数据 [Dc]Kc，存储器 1412 相当于此。因而，成为加密内容数据 [Dc]Kc 可以自由复制，但再生所需数据不能复制的结构。

另外，说明了将保持密钥的所有密钥保持部设置于安全区域，但可以只把保持秘密解密密钥的 Kmedia 保持部 1402 及 Kcard (1) 保持部 1415 配置于安全区域，保持于其它密钥保持部的密钥可以配置于可由外部参照的 ROM (Read Only Memory)。

图 41 是说明使用图 39 说明过的存储插件 200 的发布模式用的流程图，是实施例 8 的图 36 的对比图。

在图 41 中，说明了用户 1 使用存储插件 200，从内容服务器 12 接收内容数据发布时的动作。

首先，从用户 1 的便携式电话机 105，通过用户的触摸键 1108 的操作等，对存储插件 200 进行发布请求 (步骤 S400)。

由存储插件 200，从存储器 1412 中的 [KPmedia, Crtf]KPmaster 保持部 1442，经由便携式电话机 105，向内容服务器 12 发送加密数据 [KPmedia, Crtf]KPmaster (步骤 S402)。

在内容服务器 12 中，一接收加密数据 [KPmedia, Crtf]KPmaster，根据 KPmaster 保持部 324 保持的公开解密密钥 KPmaster，通过解密处理部 326 解密处理，取得公开解密密钥 KPmedia 及认证数据 Crtf (步骤 S404)。

进一步，在内容服务器 12 中，根据认证数据 Crtf 进行存储插件 200 的认证 (步骤 S406)，如果证明存储插件 200 是正式的存储插件，处理转移到 S412。

另一方面，在不被证明存储插件 200 是正式存储插件的场合，内容服务器 12 发送发布不许可通知 (步骤 S408)，便携式电话机 105

接收发布不许可通知（步骤 S410），

证明存储插件 200 是正式的存储插件的场合，在内容服务器 12 中，对话密钥发生部 314 生成对话密钥 K_s （步骤 S412）。

在内容服务器 12 中，接着，内容服务器 12 内的加密处理部 316
5 通过公开加密密钥 KP_{media} ，将对话密钥 K_s 进行加密处理，提供给数据总线 BS1（步骤 S414）。

通信装置 350 将来自加密处理部 316 的加密对话密钥 $[K_s]$ K_{media} ，通过通信网，向便携式电话机 105 的存储插件 200 发送（步骤 S416）。

10 在存储插件 200 中，解密处理部 1404 将通过存储器接口 1200 提供给数据总线 BS3 的接收数据，通过由通过数据总线 BS3 从存储器 1412 提供的秘密解密密钥 K_{media} 进行解密处理，解密抽出对话密钥 K_s （步骤 S418）。进而，在存储插件 200 中， K_{s1} 发生部 1432 生成对话密钥 K_{s1} （步骤 S420）。

15 接着，在发布模式中，首先，加密处理部 1406 通过数据总线 BS3 接收从存储器 1412 中的 $KP_{card}(1)$ 保持部 1405 提供的公开加密密钥 $KP_{card}(1)$ ，接着，转换开关 1409 变为接点 Pa 呈关闭状态，因此，加密处理部 1406 通过接点 Pa 接收由 K_{s1} 发生部 1432 提供的对话密钥 K_{s1} 。因为转换开关 1435 选择接点 Pe 关闭的状态，所以加密
20 处理部 1406 通过来自解密处理部 1404 的对话密钥 K_s ，将公开加密密钥 $KP_{card}(1)$ 及对话密钥 K_{s1} 加密，提供给数据总线 BS3（步骤 S422）。

通过便携式电话机 105，向内容服务器 12 发送由加密处理部 1406 加密的数据 $[KP_{card}(1), K_{s1}] K_s$ （步骤 S424）。

25 在内容服务器 12 中，解密处理部 318 将由通信装置 350 接收、提供给数据总线 BS1 的数据 $[KP_{card}(1), K_{s1}] K_s$ ，通过对话密钥 K_s 进行解密处理，解密抽出公开加密密钥 $KP_{card}(1)$ 及对话密钥 K_{s1} （步骤 S426）。

接着，发布控制部 312 从发布信息数据库 304 取得许可密钥 K_c
30 （步骤 S428），且以发布信息数据库 304 等保持的数据为基础，生成许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据（步骤 S430）。

加密处理部 320 接收来自发布控制部 312 的许可密钥 Kc、许可 ID 数据 License-ID 及用户 ID 数据 User-ID 等数据, 通过由解密处理部 318 提供的公开加密密钥 Kp_{card}(1) 进行加密处理(步骤 S432)。

加密处理部 322 接收由加密处理部 320 加密的数据, 再由对话密钥 K_{s1} 加密, 提供给数据总线 BS1 (步骤 S434)。

通信装置 350 将由加密处理部 322 加密的数据 [[Kc, License-ID, User-ID]K_{card}(1)]K_{s1}, 向存储插件 200 发送 (步骤 S436)。

在存储插件 200 中, 转换开关 1435 被转换为选择接点 Pf 呈关闭状态的状态, 因此, 解密处理部 1410 通过来自 K_{s1} 发生部 1432 的对话密钥 K_{s1} 进行解密处理, 抽出数据 [Kc, License-ID, User-ID]K_{card}(1) (步骤 S438)。

进一步, 在存储插件 200 中, 解密处理部 1416 根据来自存储器 1412 中 K_{card}(1) 保持部 1415 的输出, 将来自解密处理部 1410 的数据 [Kc, License-ID, User-ID]K_{card}(1) 解密, 将解密的许可 ID 数据 License-ID、用户 ID 数据 User-ID、许可密钥 Kc 存入存储器 1412 中的寄存器 1500 (步骤 443)。

另一方面, 内容服务器 12 从发布信息数据库 304 取得加密内容数据 [Dc]Kc, 通过通信装置 350 向存储插件 180 发送 (步骤 S444)。

在存储插件 200 中, 将接收的加密内容数据 [Dc]Kc 直接存入存储器 1412 (步骤 S446)。

通过以上动作, 存储插件 200 变为内容数据可再生的状态。

图 42 是说明在便携式电话机 105 内, 从保持于实施例 9 的存储插件 200 的加密内容数据, 将内容数据解密, 作为音乐向外部输出用的再生处理的流程图, 是实施例 8 的图 37 的对比图。

参照图 41, 当根据来自便携式电话机的触摸键 1108 等的用户 1 的指示, 一向便携式电话机 105 提供再生请求时 (步骤 S500), 从便携式电话机 105 向存储插件 200 发送加密数据 [K_{Pp}, Crtf]K_{Pmaster} (步骤 S502)。

在存储插件 200 中, 通过由在解密处理部 1452 的公开解密密钥 K_{Pmaster} 进行解密处理, 取得公开加密密钥 K_{Pp} 及认证数据 Crtf (步骤 S504)。控制器 1420 根据认证数据 Crtf 认证便携式电话机 105 是否是正式设备 (步骤 S506), 当证明是正式设备, 处理转移到步

骤 S508, 当不被证明是正式设备时, 向便携式电话机 105 发送再生不许可通知 (步骤 S544)。

证明便携式电话机 105 是正式设备的场合 (步骤 S506), 对话密钥发生部 1432 生成对话密钥 $Ks1$ (步骤 S508)。加密处理部 1430 根据来自解密处理部 1452 的公开加密密钥 KPp , 将对话密钥 $Ks1$ 加密 (步骤 S510), 从存储插件 200 向便携式电话机 105 发送加密对话密钥 $[Ks1]Kp$ (步骤 S512)。

在便携式电话机 105 中, 通过在解密处理部 1522 的解密处理, 解密抽出对话密钥 $Ks1$ (步骤 S514)。接着, 在对话密钥发生部 1502 中, 生成对话密钥 Ks (步骤 S516), 加密处理部 1504 通过对话密钥 $Ks1$ 将对话密钥 Ks 加密 (步骤 S518), 从便携式电话机 105 向存储插件 200 发送加密对话密钥 $[Ks]Ks1$ (步骤 S520)。

在存储插件 200 中, 解密处理部 1410 通过对话密钥 $Ks1$, 将加密对话密钥 $[Ks]Ks1$ 进行解密处理, 抽出对话密钥 Ks (步骤 S522)。进而, 在存储插件 200 中, 控制器 1420 从存储器 1412 中的寄存器 1500 读出许可 ID 数据 License-ID、用户 ID 数据 User-ID 等 (步骤 S524)。

控制器 1420 根据含于许可 ID 数据 License-ID 等的信息, 判断由许可 ID 数据 License-ID 中的数据指定的内容数据 (音乐数据) 再生处理的累计数是否超过可以再生次数的上限值 (步骤 S526), 判断为没有超过可以再生次数的场合, 存储插件 200 按照进行再生处理, 更新存储器 1412 中的寄存器 1500 中的许可 ID 数据 License-ID 内的再生处理累计数方面的数据 (步骤 528)。

接着, 存储插件 200 从存储器 1412 读出许可密钥 Kc , 通过在步骤 S522 抽出的对话密钥 Ks , 将许可密钥 Kc 加密 (步骤 S532), 将加密许可密钥 $[Kc]Ks$ 提供给数据总线 BS2 (步骤 S534)。

便携式电话机 105 的解密处理部 1506 通过由对话密钥 Ks 进行解密处理, 取得许可密钥 Kc (步骤 S536)。

接着, 存储插件 200 从存储器 1412 读出加密内容密钥 $[Dc]Kc$, 提供给数据总线 BS2 (步骤 S538)。

便携式电话机的音乐再生部 1508 将加密内容密钥 $[Dc]Kc$, 通过抽出的许可密钥 Kc 进行解密处理 (步骤 S540), 再生内容数据, 提

供给混合部 1510 (步骤 S542)。

另一方面,在步骤 S526 中,判断为控制器 1420 解密处理不可能的场合,存储插件 200 向便携式电话机 105 发送再生不许可通知(步骤 S544)。

- 5 按照上述结构,存储插件及便携式电话机即使生成独自の对话密钥的场合,也能够限制用户可再生内容数据的次数。

图 43 是说明在实施例 9 的 2 个存储插件间,内容数据及密钥数据等移动模式用的流程图,是实施例 8 的图 38 的对比图。

- 参照图 43,首先,在图 43 中,设定便携式电话机 105 为发送侧,10 与其结构相同的便携式电话机 107 为接收侧。另外,便携式电话机 107 中也装有与存储插件 200 结构相同的存储插件 202。

便携式电话机 105 首先向插入接收侧便携式电话机 107 的存储插件 202 输出移动请求(步骤 S600)。

- 由此,从装于便携式电话机 107 的存储插件 202 向存储插件 20015 发送加密数据[KPmedia, Crtf]KPmaster(步骤 S602)。

在存储插件 200 中,一接收加密数据[KPmedia, Crtf]KPmaster 时,根据 KPmaster 保持部 1450 保持的公开解密密钥 KPmaster,通过解密处理部 1452 的解密处理,取得公开加密密钥 KPmedia 及认证数据 Crtf(步骤 S604)。

- 20 进一步,在存储插件 200 中,根据认证数据 Crtf 进行存储插件 202 的认证(步骤 S606),如果证明存储插件 202 是正式存储插件,处理转移到 S612。另一方面,不被证明存储插件 202 是正式存储插件的场合,存储插件 200 发送移动不许可通知(步骤 S608),便携式电话机 107 接收移动不许可通知(步骤 S610)。

- 25 证明存储插件 202 是正式存储插件的场合,在存储插件 200 中,对话密钥发生部 1432 生成对话密钥 Ks1(步骤 S612)。

在存储插件 200 中,接着,加密处理部 1430 通过公开加密密钥 KPmedia,将对话密钥 Ks1 进行加密处理,提供给数据总线 BS3(步骤 S614)。

- 30 从存储插件 200,将来自加密处理部 1430 的加密对话密钥 [Ks]Kmedia,通过便携式电话机 105,向便携式电话机 107 的存储插件 202 发送(步骤 S616)。

在存储插件 202 中,解密处理部 1404 将通过存储器接口 1200 提供给数据总线 BS3 的接收数据,通过由秘密解密密钥 Kmedia 进行解密处理,解密抽出对话密钥 Ks(步骤 S618)。进而,在存储插件 202 中,与 Ks1 发生器 1432 结构相同的 Ks2 发生部 1432' 生成对话密钥 Ks2(步骤 S620)。

接着,在存储插件 202 中,首先,加密处理部 1406 通过数据总线 BS3 接收从存储器 1412 中的 KPcard(1) 保持部 1405 提供的公开加密密钥 KPcard(1),转换开关 1409 变为接点 Pa 呈关闭状态,因此,加密处理部 1406 通过接点 Pa,接收由 Ks2 发生部 1432' 提供的对话密钥 Ks2。因为转换开关 1435 选择接点 Pe 关闭的状态,因此,加密处理部 1406 通过来自解密处理部 1404 的对话密钥 Ks1,将公开加密密钥 KPcard(1) 及对话密钥 Ks2 加密,提供给数据总线 BS3(步骤 S622)。

通过便携式电话机 107 向存储插件 200 发送由加密处理部 1406 加密的数据[KPcard(1)、Ks2] Ks1(步骤 S624)。

在存储插件 200 中,解密处理部 1410 将从存储插件 202 发送的加密数据,通过对话密钥 Ks1 解密,解密抽出存储插件 202 的公开加密密钥 KPcard(2) 及对话密钥 Ks2(步骤 S626)。这时,在转换开关 1435,接点 Pf 关闭,来自 Ks1 发生电路 1432 的对话密钥 Ks1 被提供给解密处理部 1410。

接着,在存储插件 200 中,从存储器 1412 中的寄存器 1500,读出许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID(步骤 S629)。

进一步,存储插件 200 的加密处理部 1414 通过在解密处理部 1410 抽出的存储插件 202 中的公开加密密钥 KPcard(2),将许可密钥 Kc、许可 ID 数据 License-ID、用户 ID 数据 User-ID 加密(步骤 S634)。

由存储插件 200 加密处理部 1414 加密的数据,通过转换开关 1409(接点 Pd 关闭),再被提供给加密处理部 1406,加密处理部 1406 通过存储插件 202 的对话密钥 Ks2,将数据[Kc, License-ID, User-ID]Kcard(2) 加密(步骤 S636)。这时,转换开关 1435 接点 Pg 关闭,来自解密处理电路 1410 的对话密钥 Ks2 被提供给加密处理部 1406。

接着，存储插件 200 通过便携式电话机 105，向存储插件 202 发送加密的数据 $[[Kc, License-ID, User-ID]Kcard(2)]Ks2$ (步骤 S638)。

5 在存储插件 202 中，将从存储插件 200 发送的数据通过解密处理部 1410，根据对话密钥 $Ks2$ 进行解密处理 (步骤 S641)。进而，存储插件 202 根据秘密解密密钥 $Kcard(2)$ ，将数据 $[Kc, License-ID, User-ID]Kcard(2)$ 解密，将解密的许可密钥 Kc 、许可 ID 数据 $License-ID$ 、用户 ID 数据 $User-ID$ 存入存储器 1412 中的寄存器 1500 (步骤 S643)。

10 另一方面，存储插件 200 从寄存器 1500 将许可密钥 Kc 、许可 ID 数据 $License-ID$ 、用户 ID 数据 $User-ID$ 消除 (步骤 S644)，将加密内容数据 $[Dc]Kc$ 从存储器 1412 读出，向存储插件 202 发送 (步骤 S646)。

15 存储插件 202 将接收的加密内容数据直接存入存储器 1412 (步骤 S648)。

即，按照上述结构也能实现与实施例 8 相同的动作。

20 另外，在以上说明的各实施例中，作为发布数据附带于内容数据的非加密数据，比如关于上述音乐数据的曲名、表演者 (歌手、演奏家等)、作曲家、作词家等有关该音乐数据 (内容数据) 的版权数据或访问音乐服务器 30 的信息等，也可以作为附加信息 Di 与加密内容数据一起发布。该附加数据 Di ，为了能在发布、移动、复制中与内容数据一起被处理，再生时分离，与内容数据分开访问，与加密内容数据被记录于同一存储器 1412 中。

25 以上对该发明进行了详细说明，但这仅是例示用的，不是限定，发明的精神和范围只通过附带的权利要求加以限定，请深刻理解。

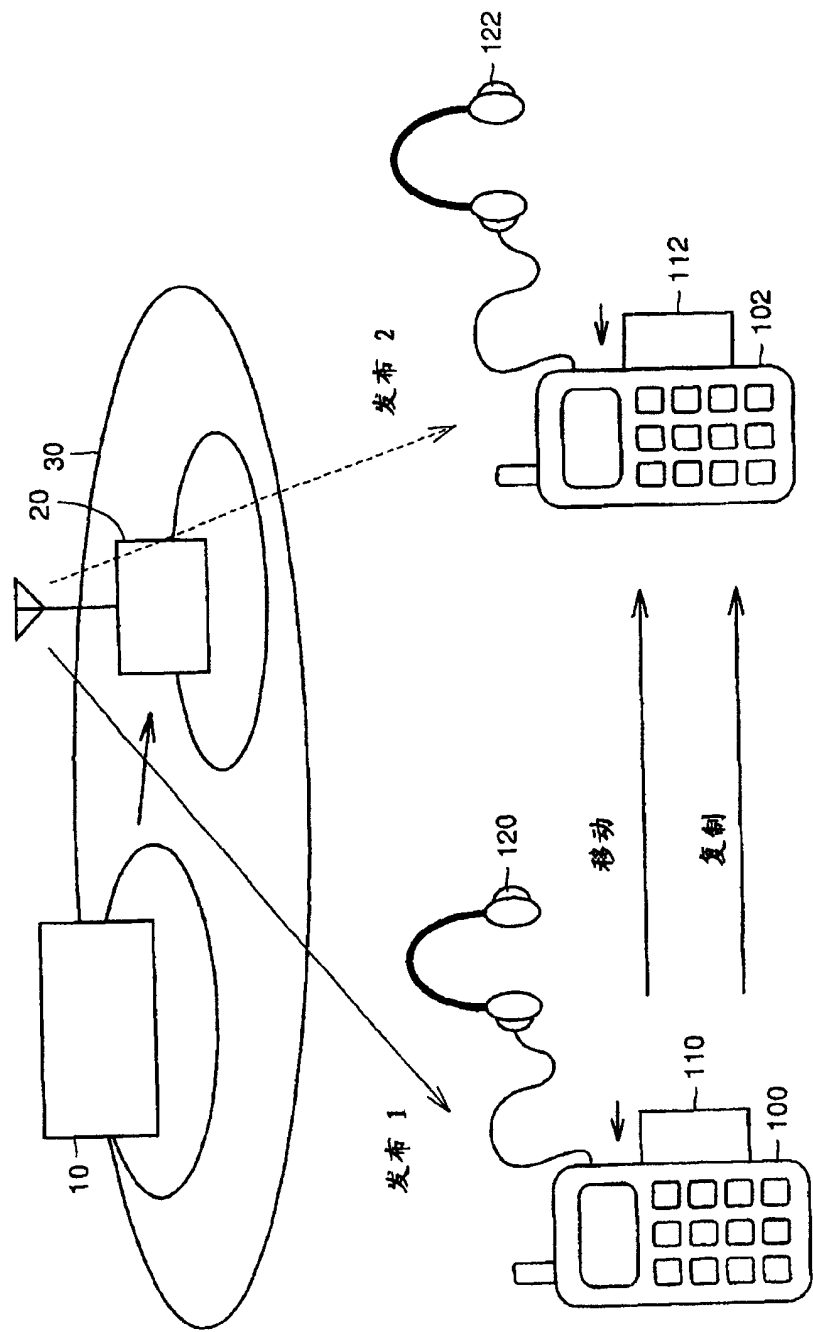
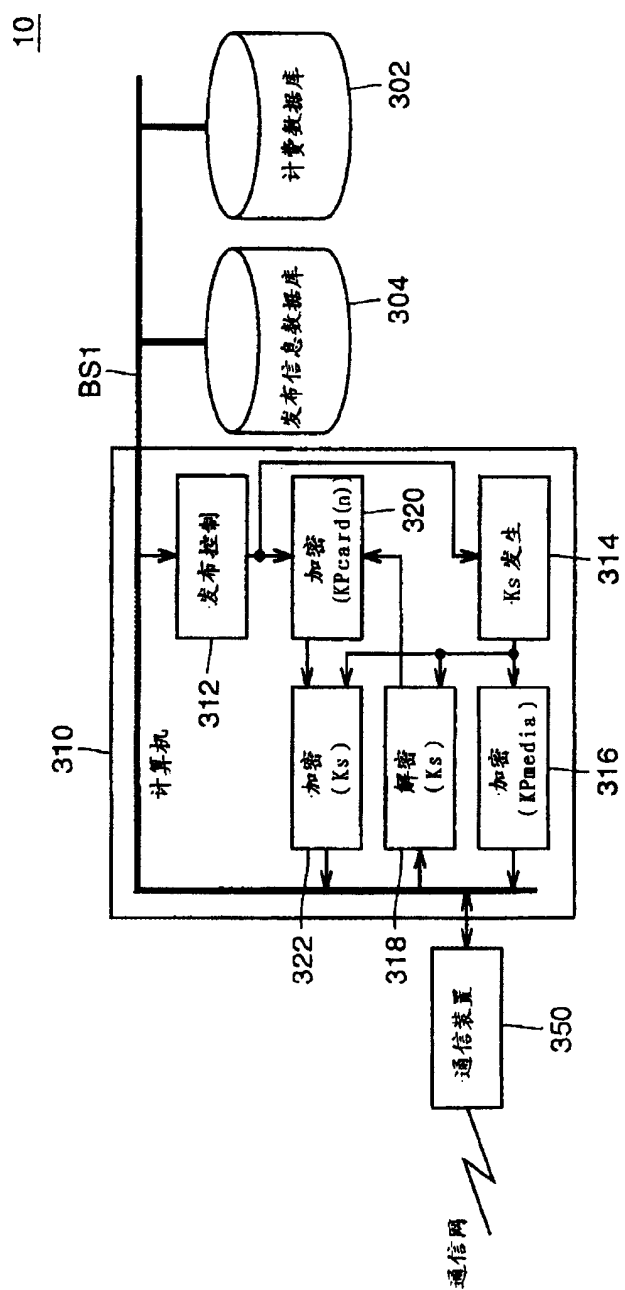


图 1

	符号	属性	特性	
			媒体固有	在所有存储插件通用
存储插件 内部管理密钥	Kmedia	秘密解密密钥		每个存储插件不同
	Kcard(n)	秘密解密密钥		
	KPcard(n)	公开加密密钥		与 Kcard (n) 成对 由 KPcard (n) 加密的数据可由 Kcard (n) 解密
存储插件 外管理密钥	KPmedia	公开加密密钥	媒体固有	与 Kmedia 成对 由 KPmedia 加密的数据可由 Kmedia 解密
	Ks	公用密钥	对话固有	每次通信 (例: 每次访问) 发生, 由发布服务器、便携式电话机管理
发布数据	Kc	公用密钥	许可密钥	加密内容数据的解密密钥
	License-ID	有关再生的信息		例: 乐曲名的特定信息 再生次数的限制信息
	User-ID	识别接收者的信息		例: 电话号码
	Dc	内容数据		例: 音乐信息数据
	[Dc]Kc	加密内容数据		由公用密钥 Kc 加密的内容数据

图 2



3 图

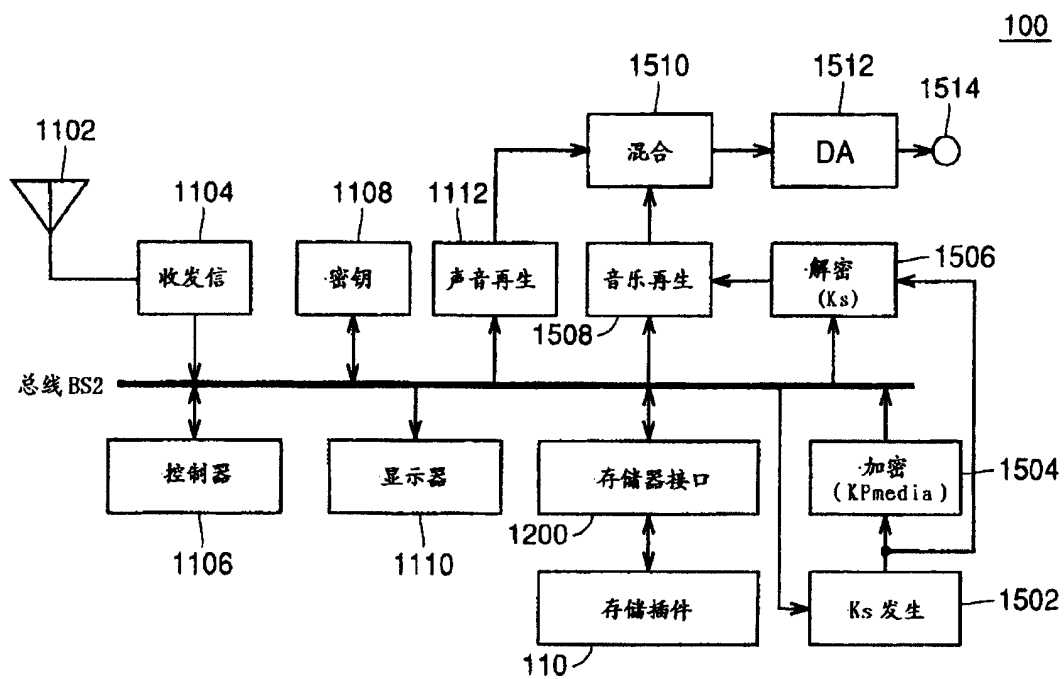


图 4

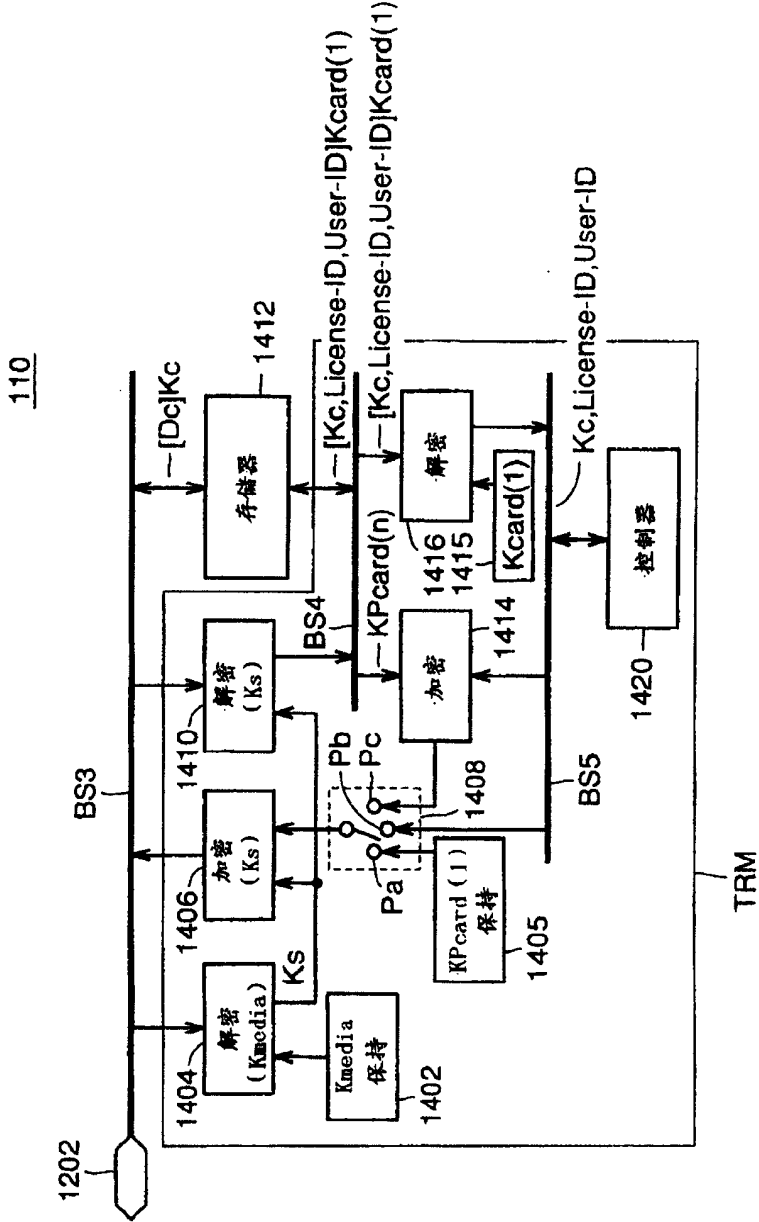


图 5

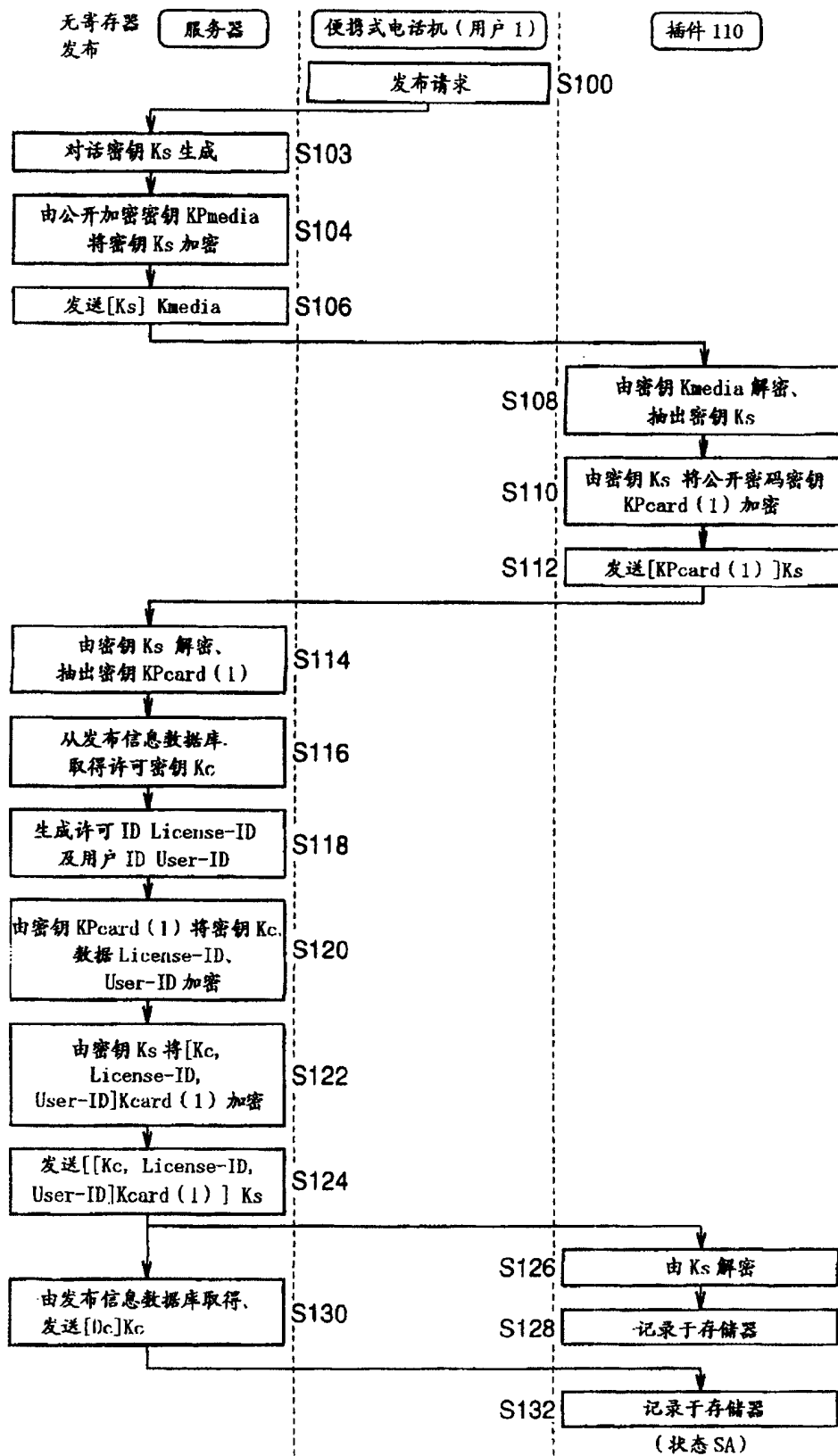


图 6

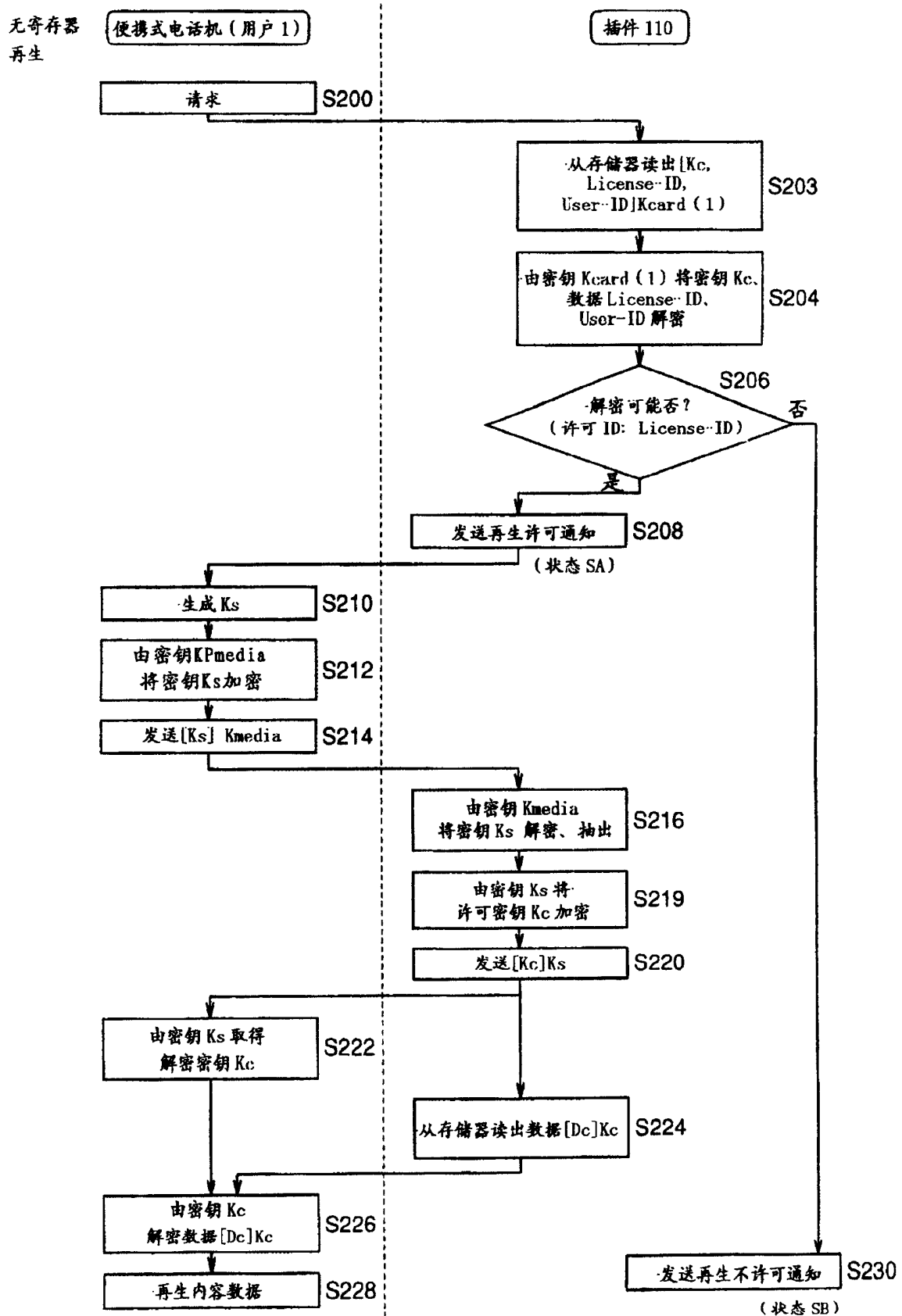


图 7

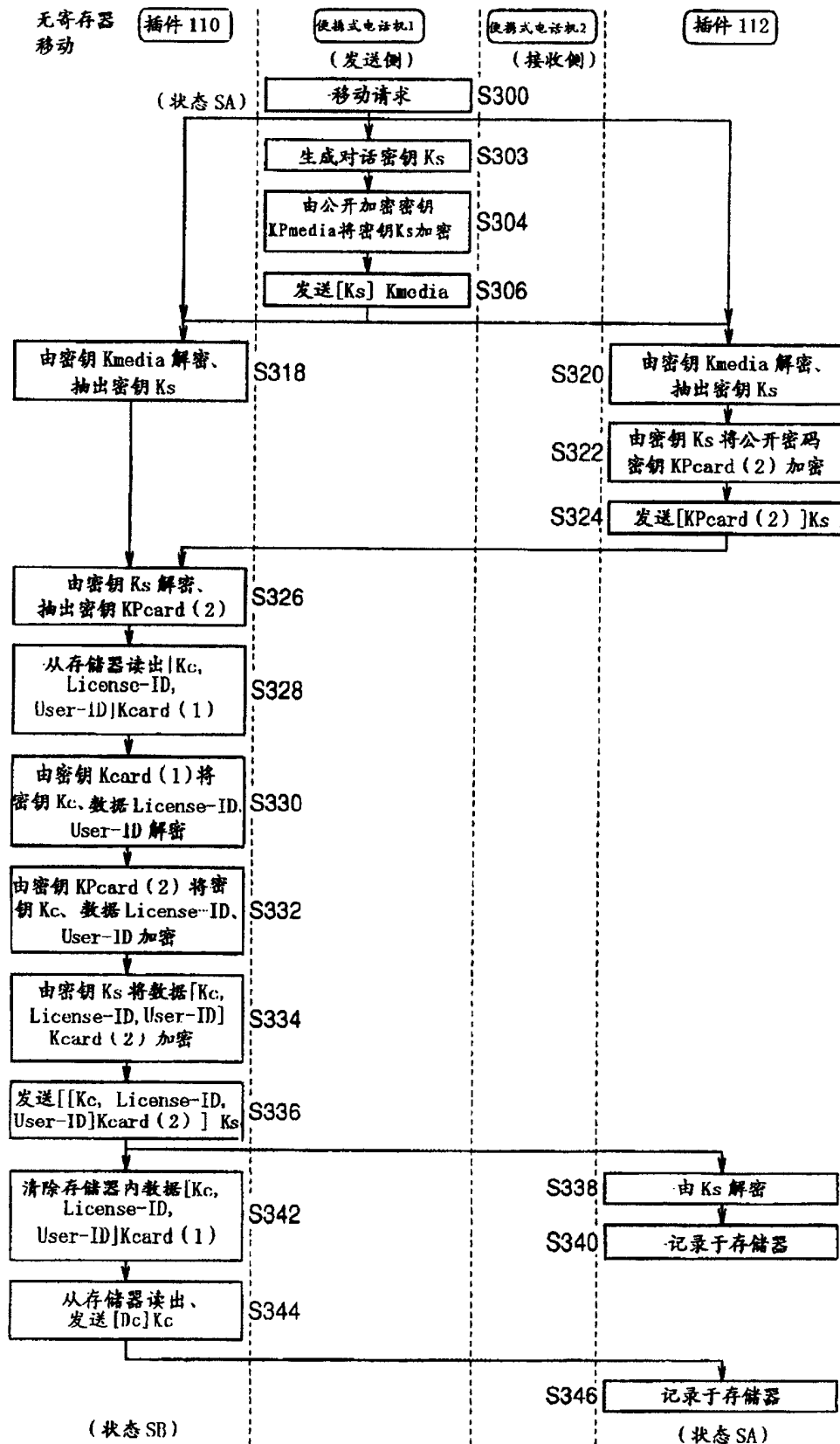


图 8

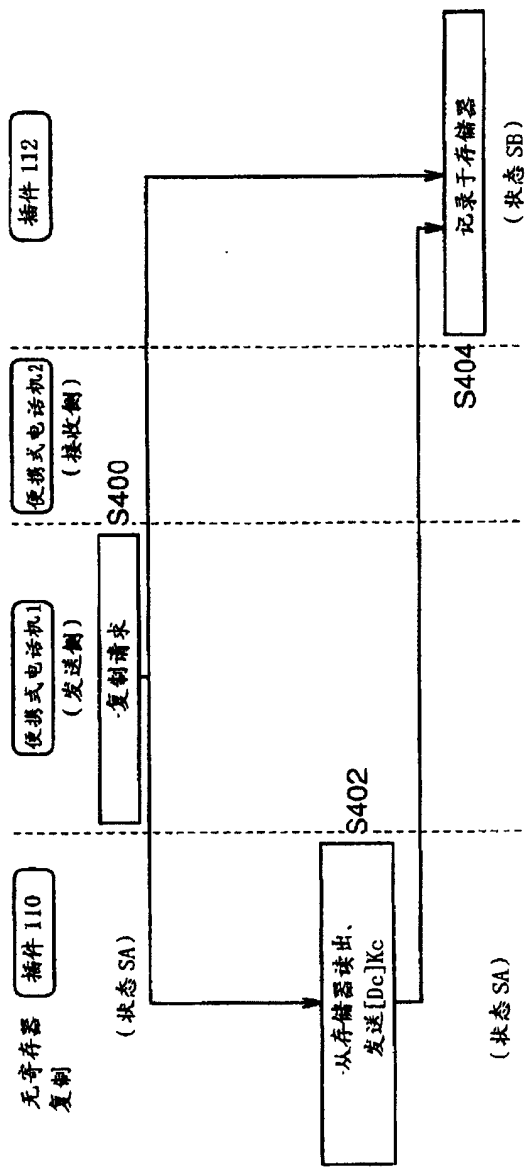


图 9

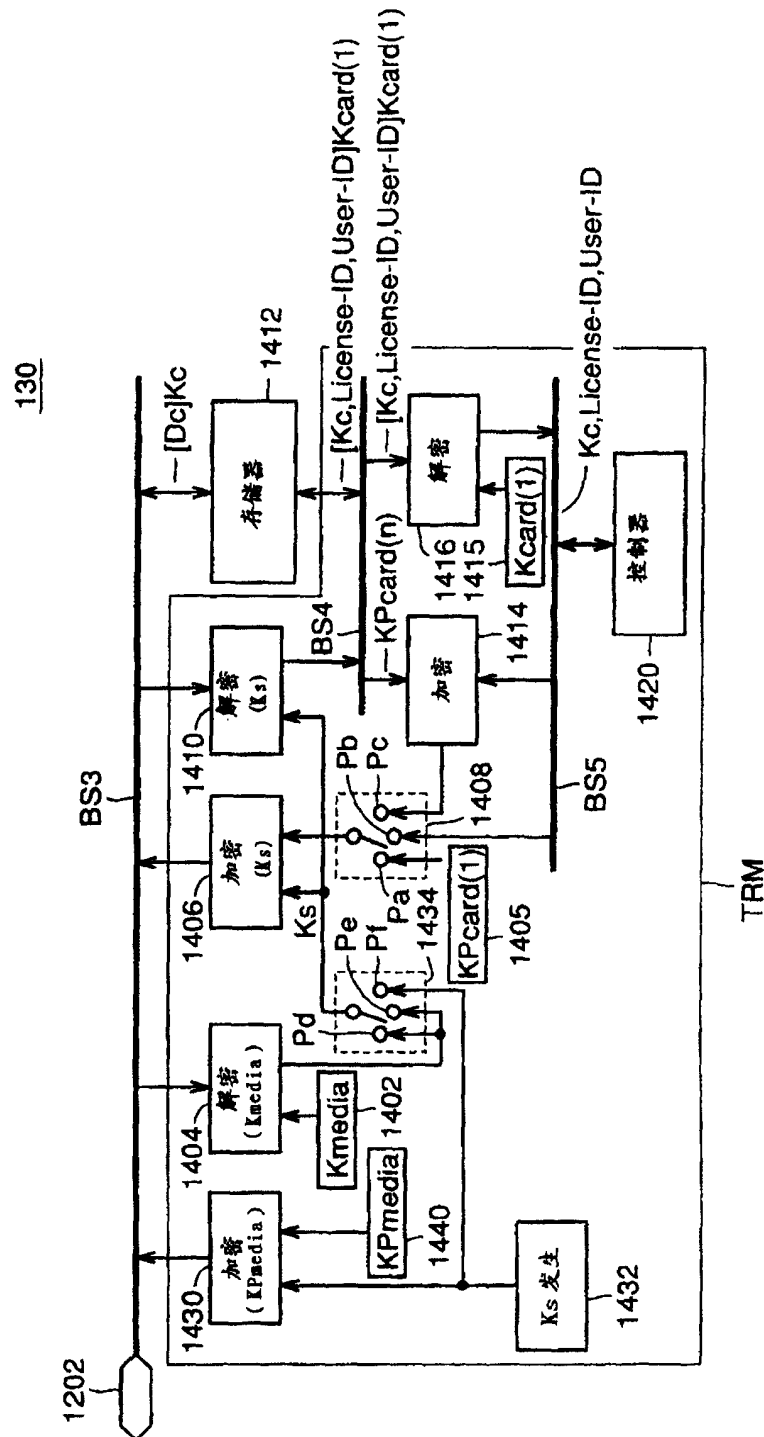


图 10

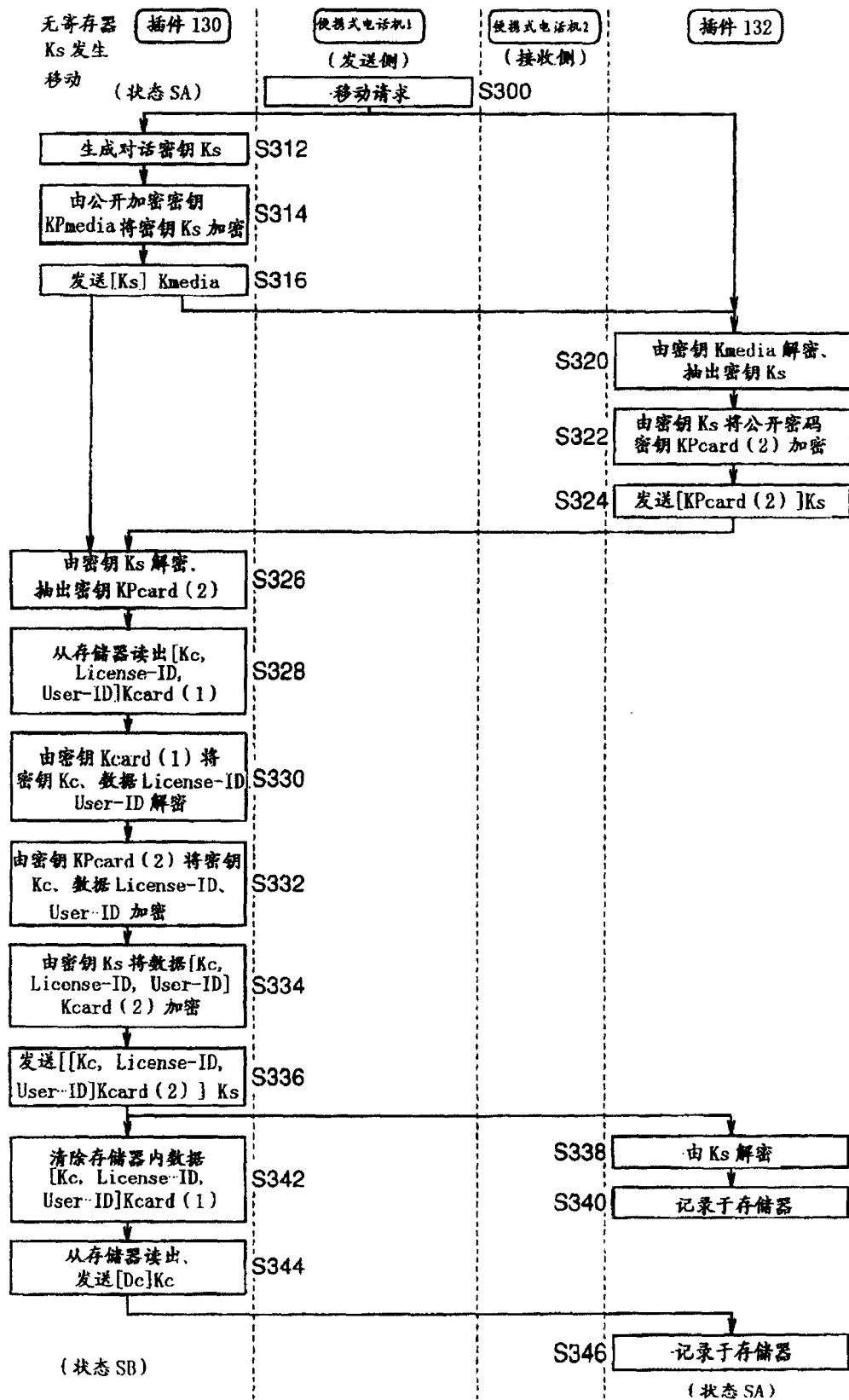
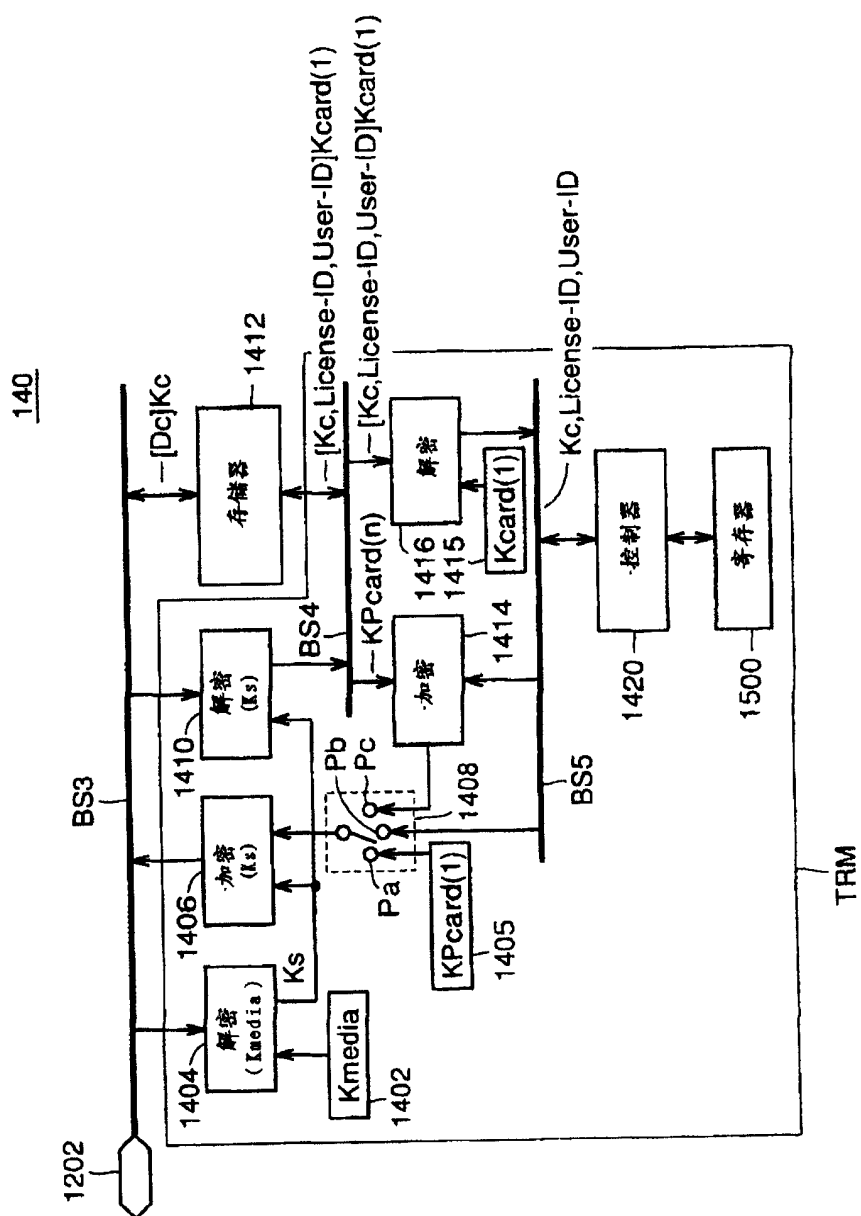


图 11



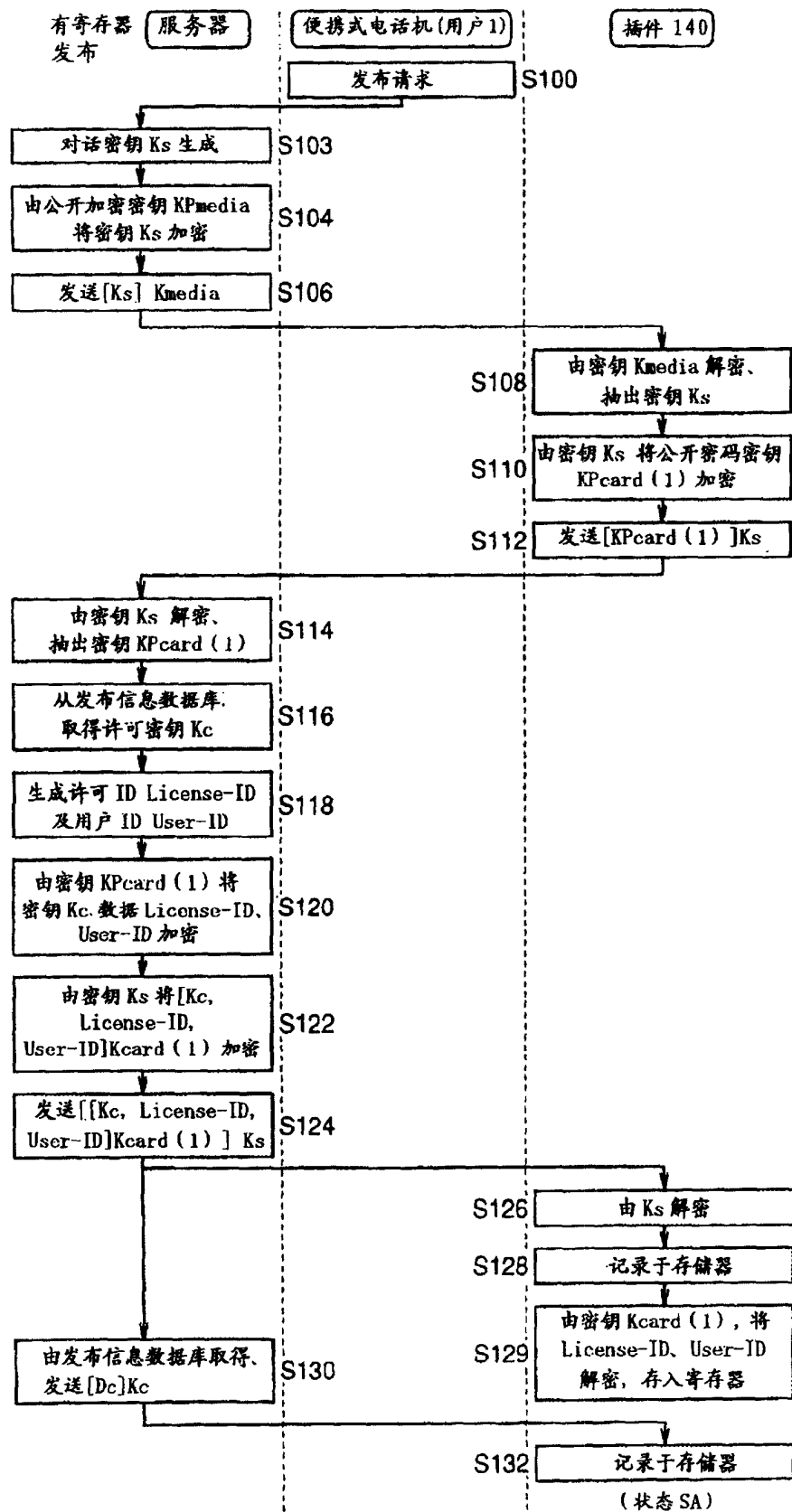


图 13

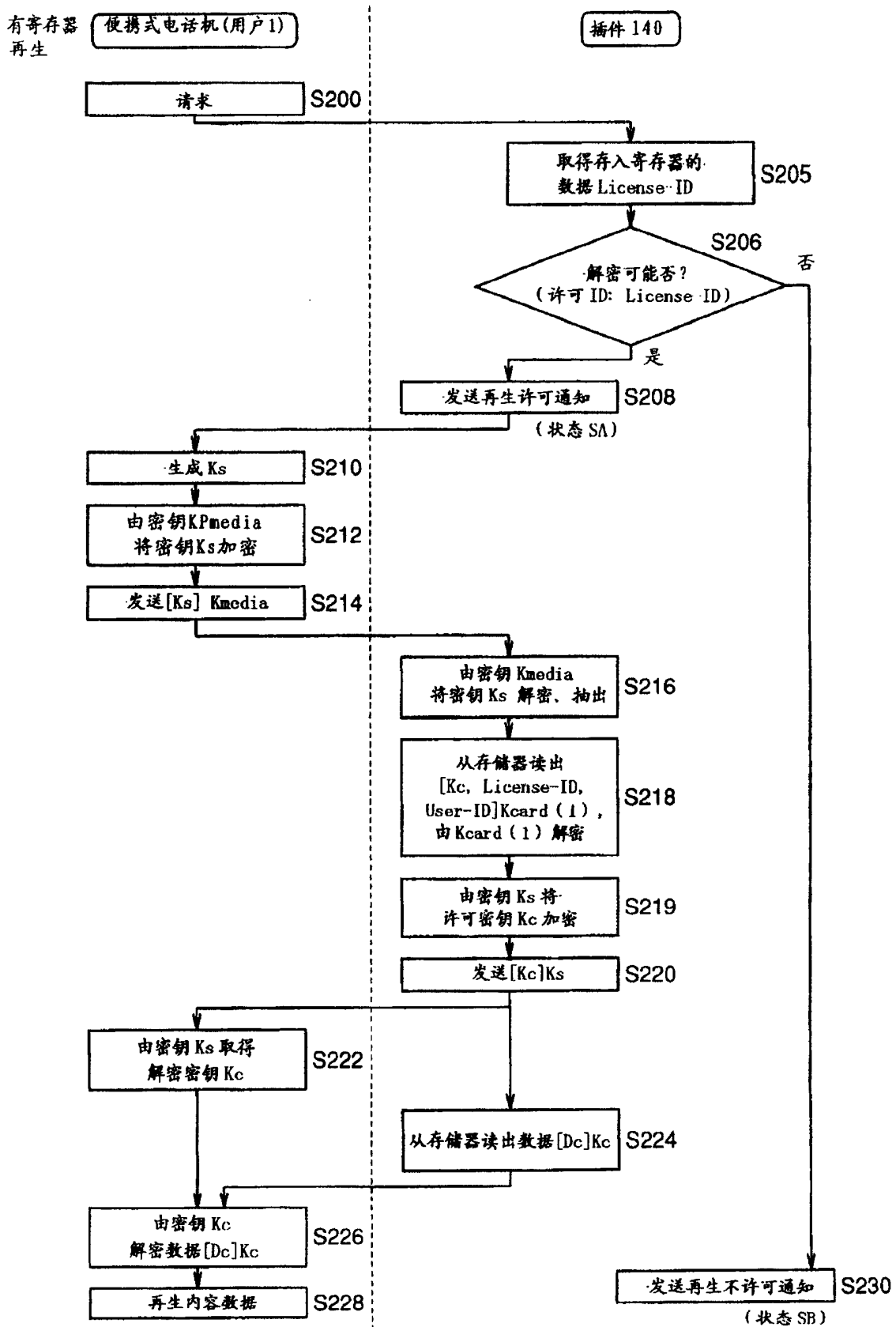


图 14

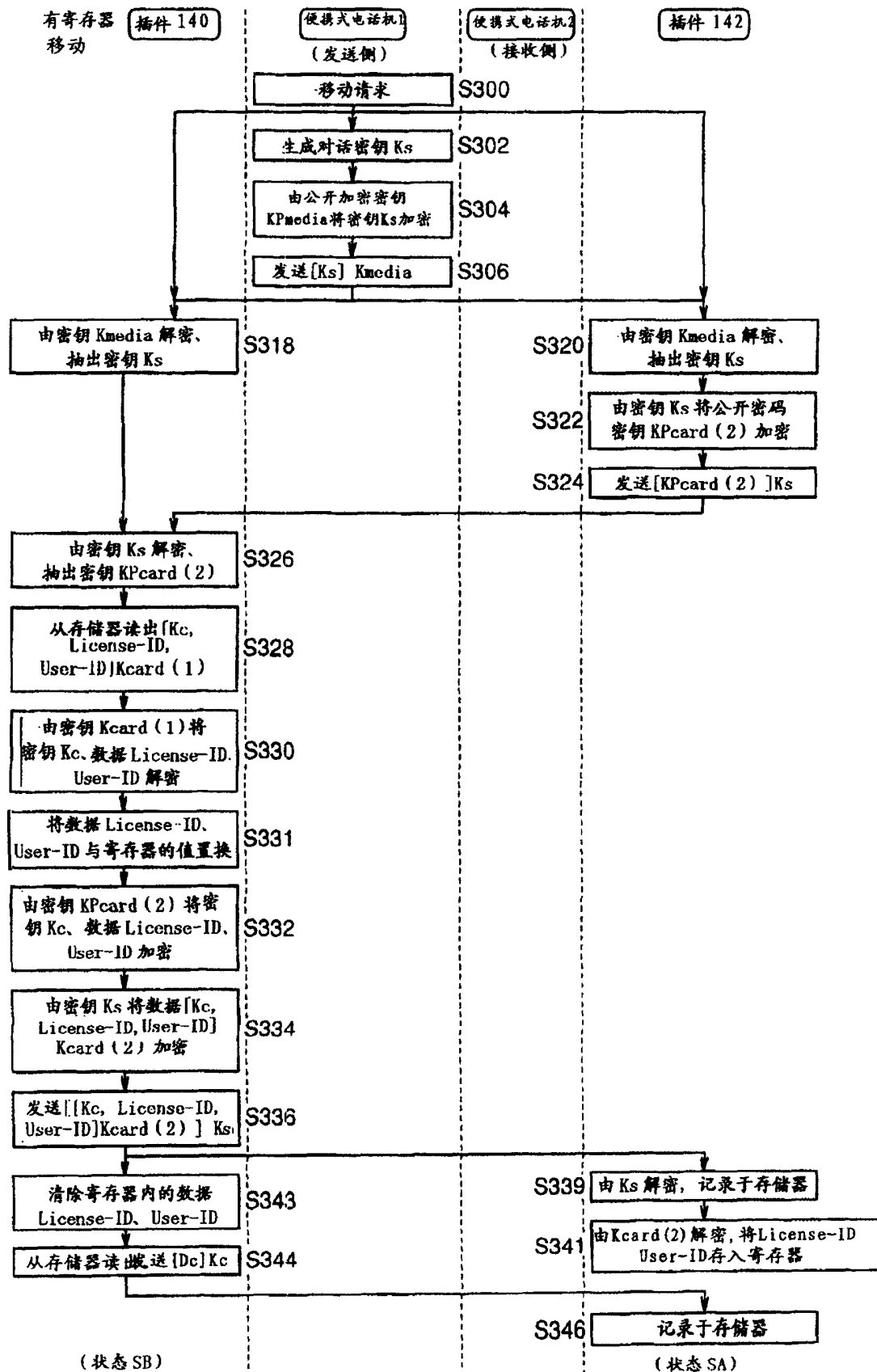


图 15

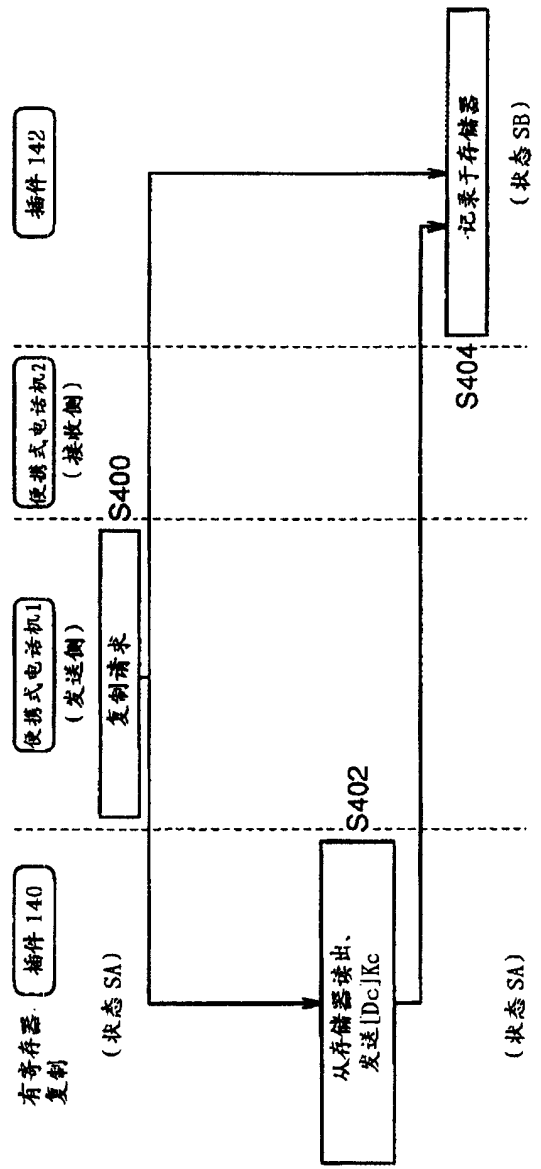


图 16

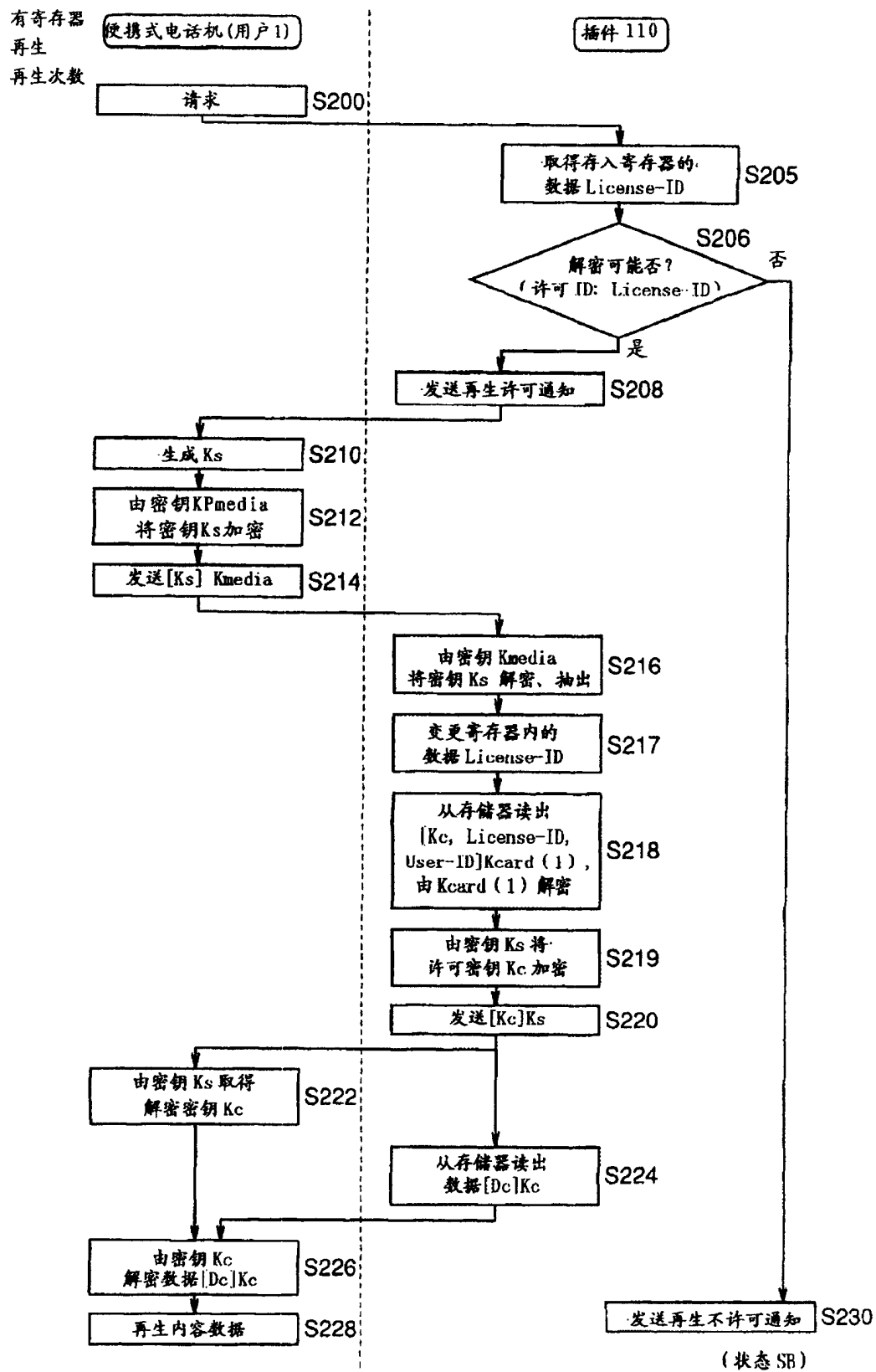
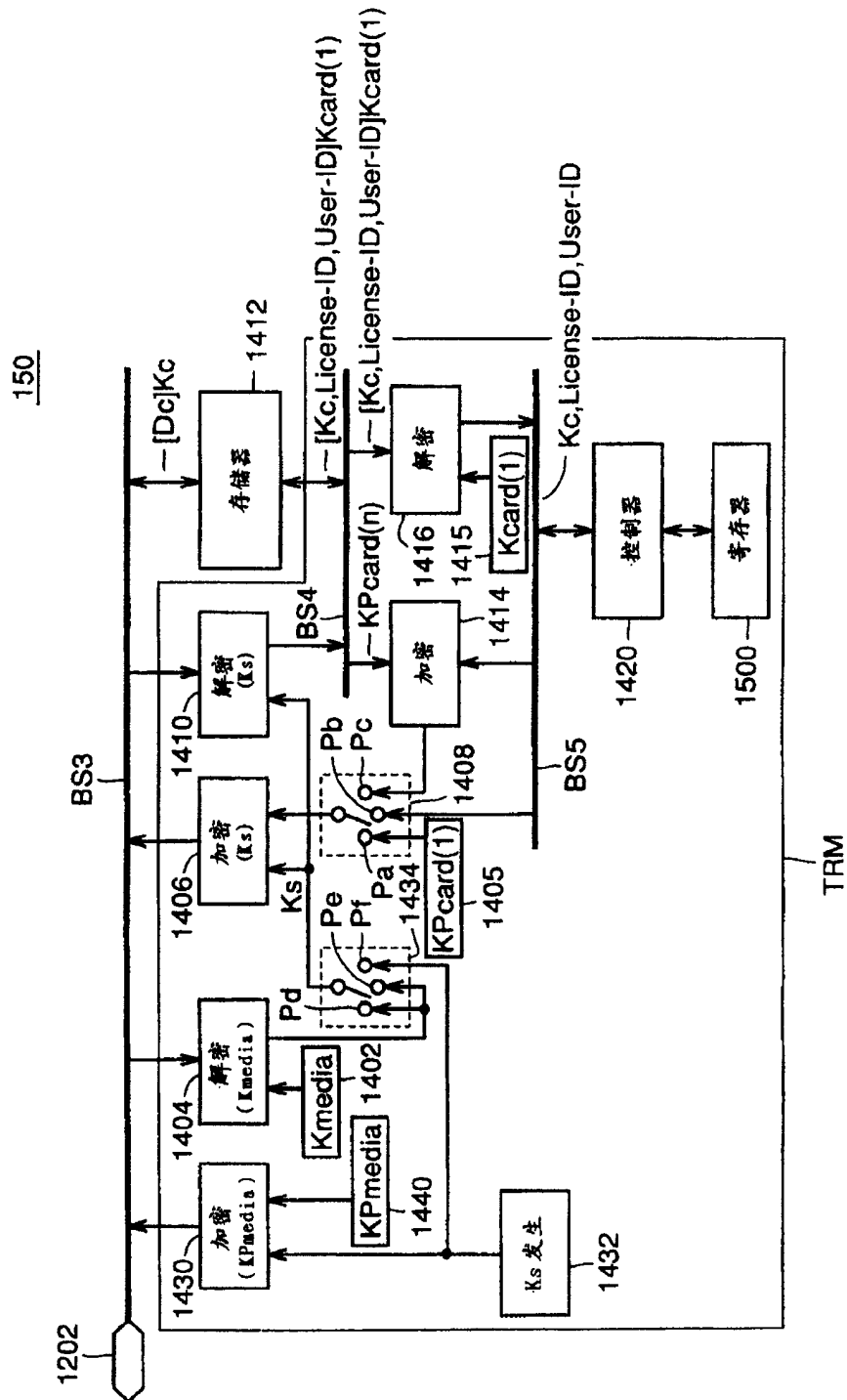


图 17



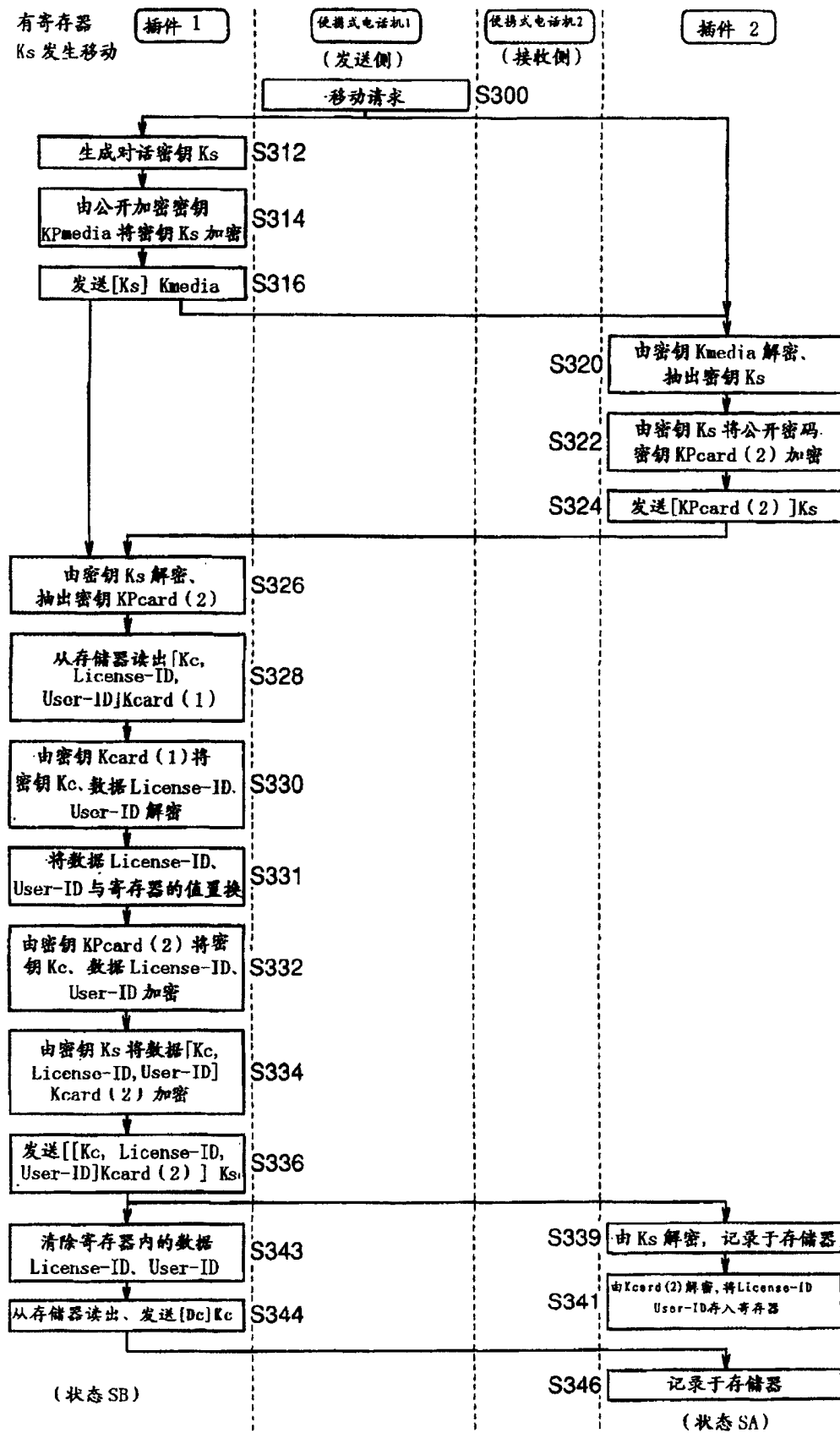


图 19

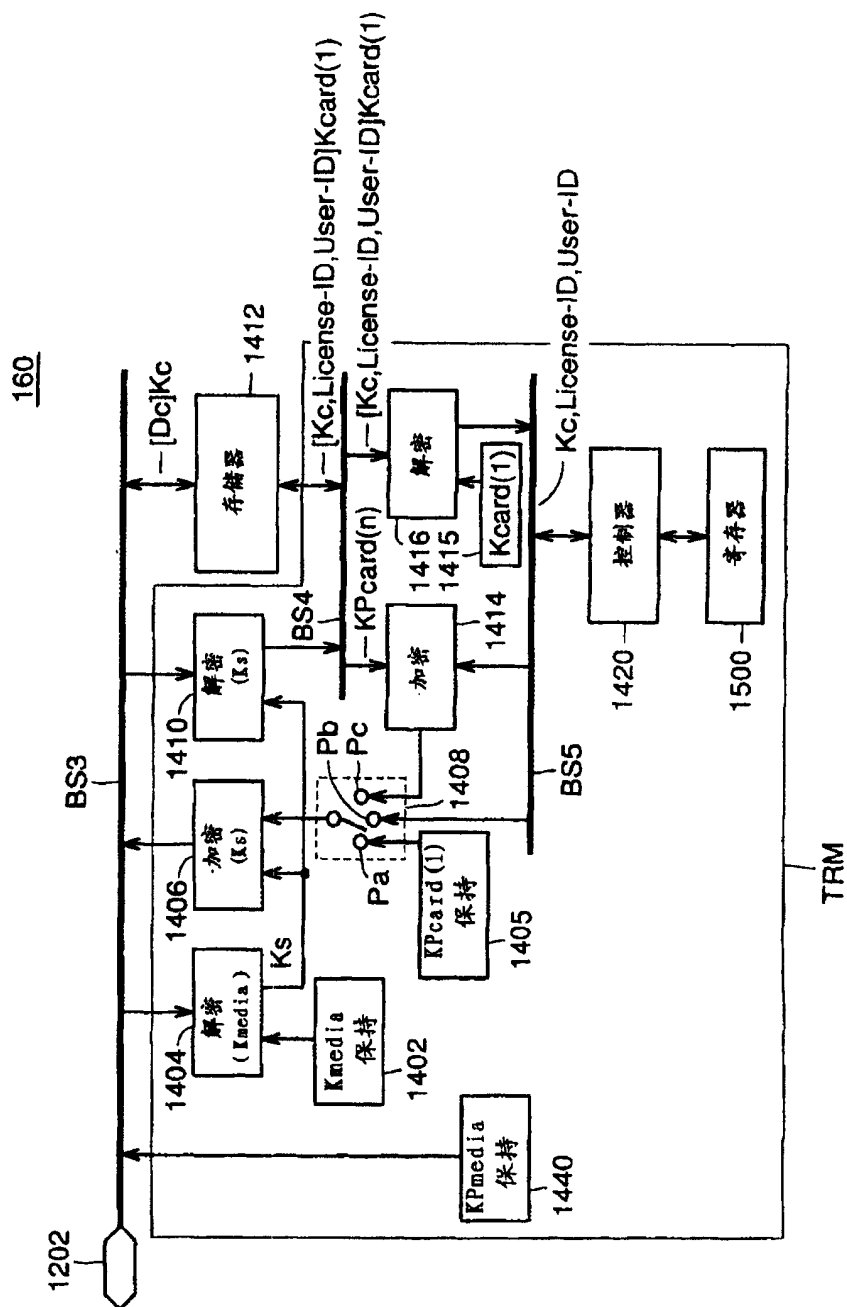


图 20

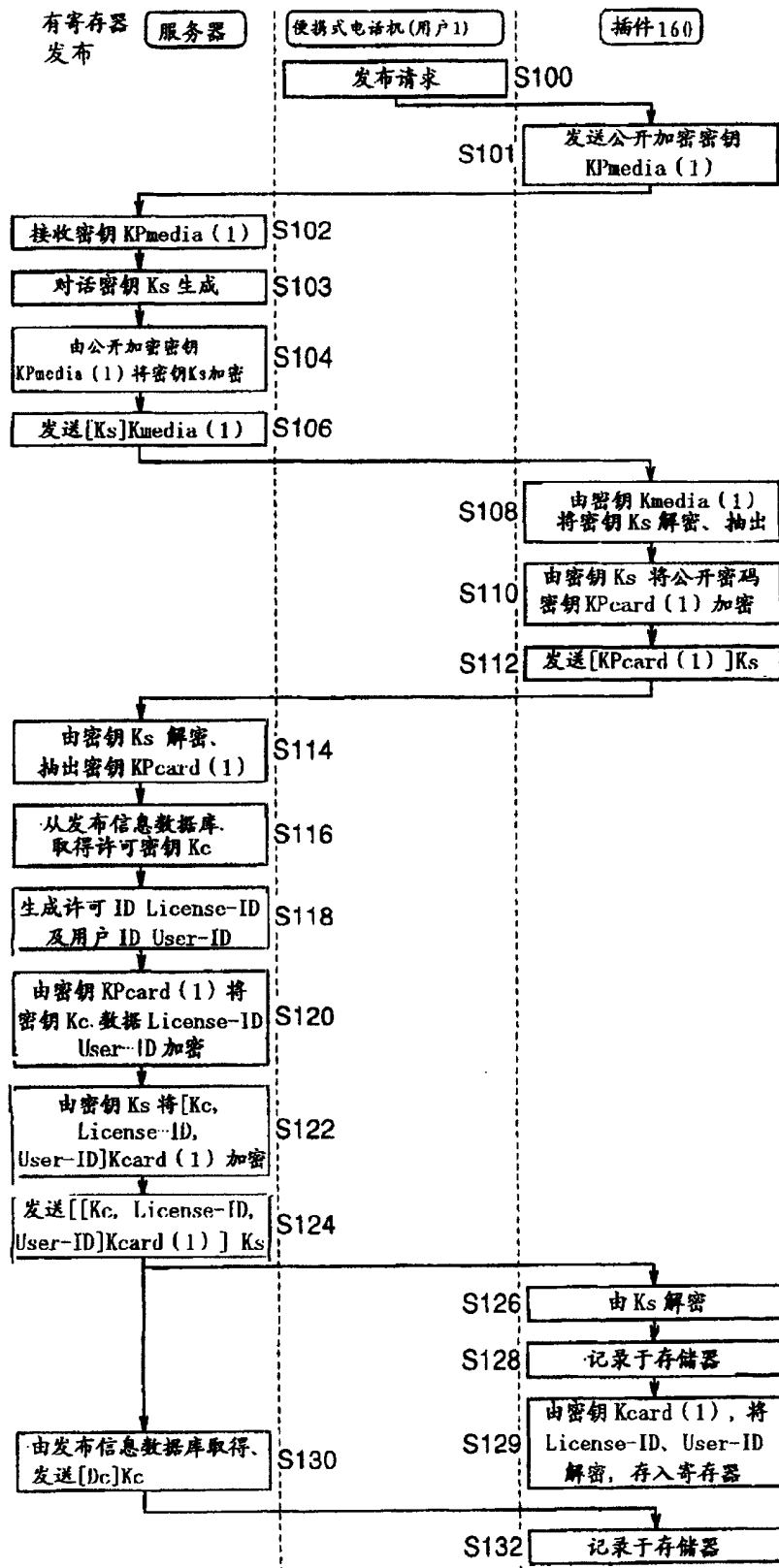


图 21

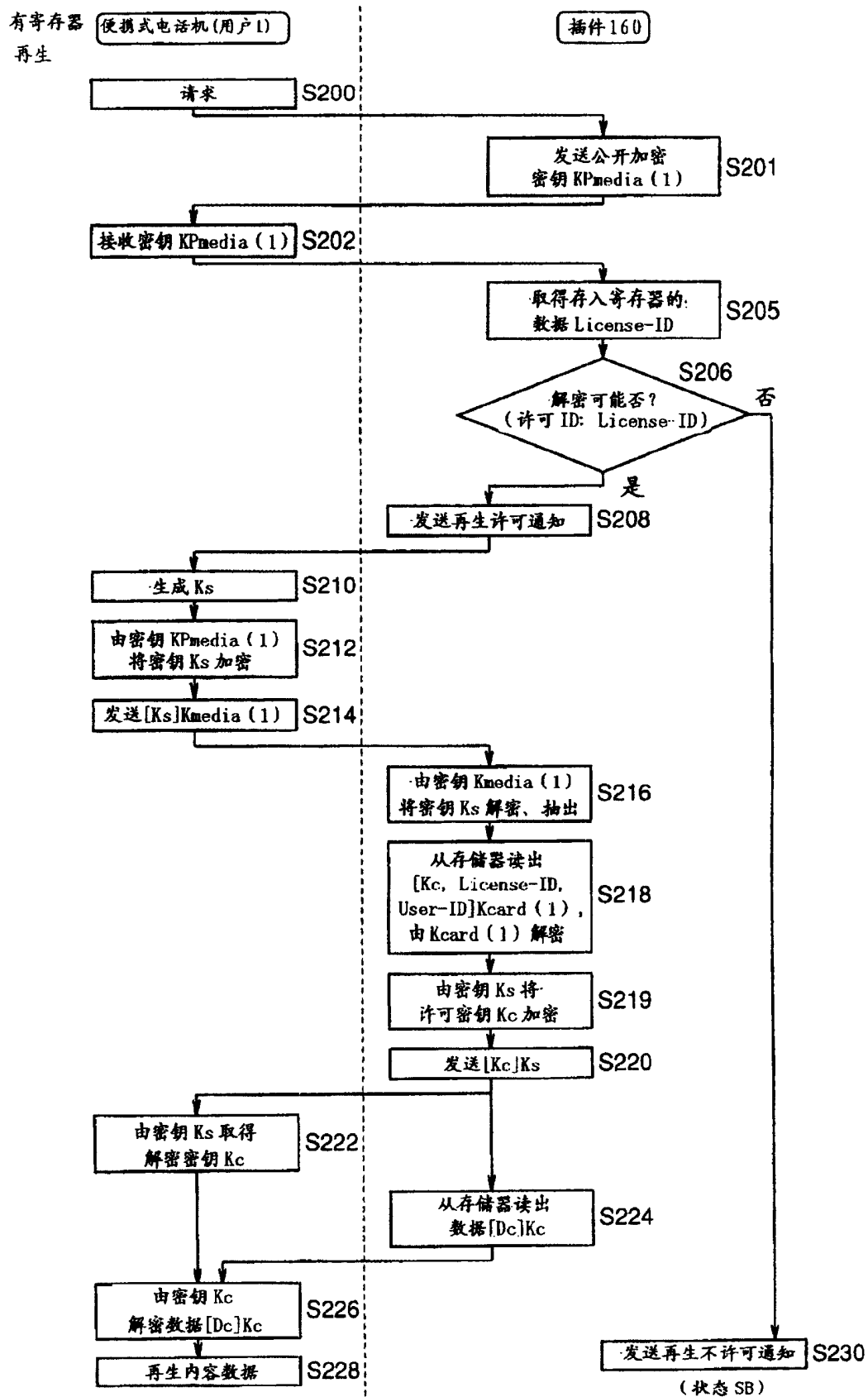
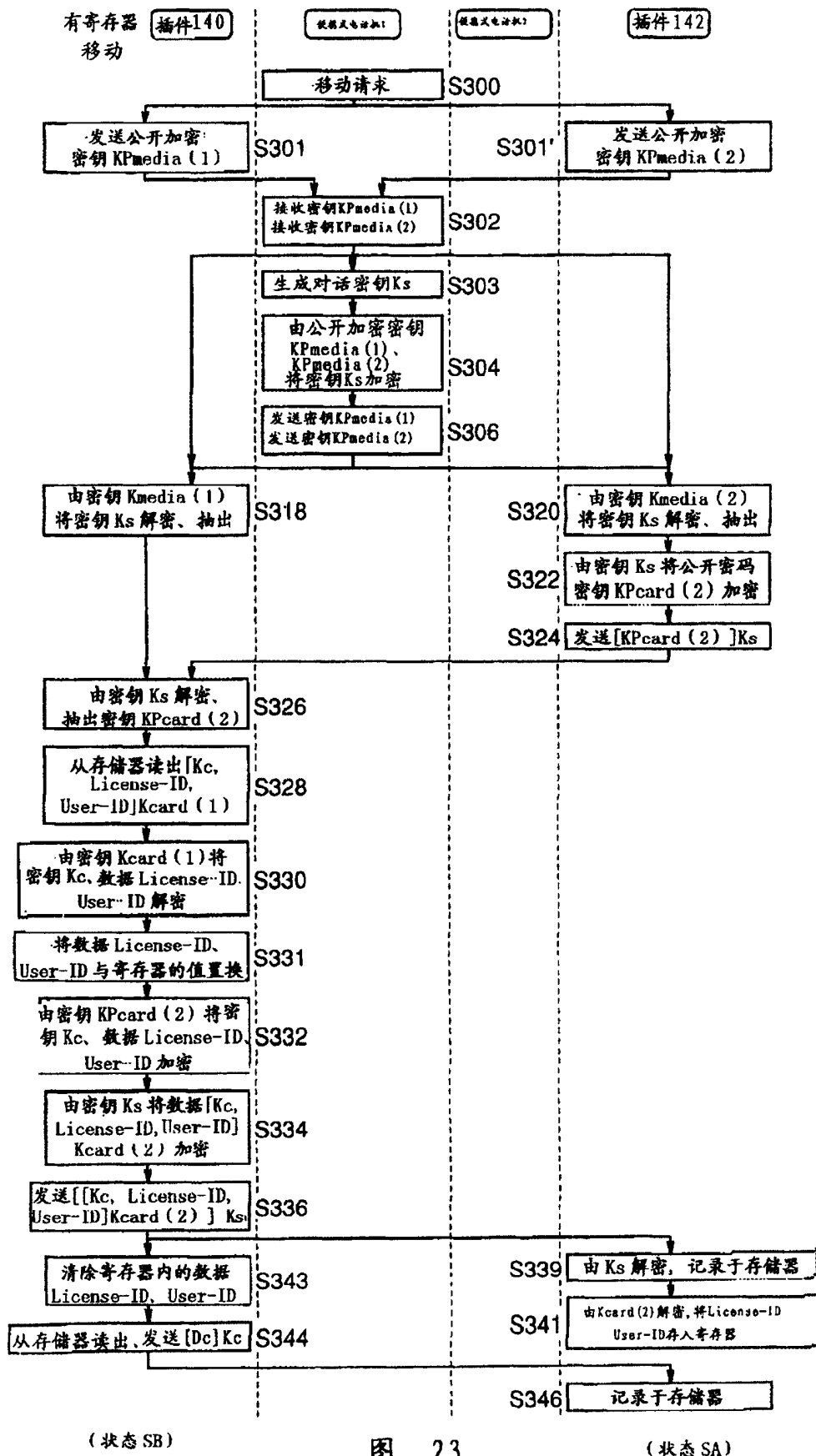
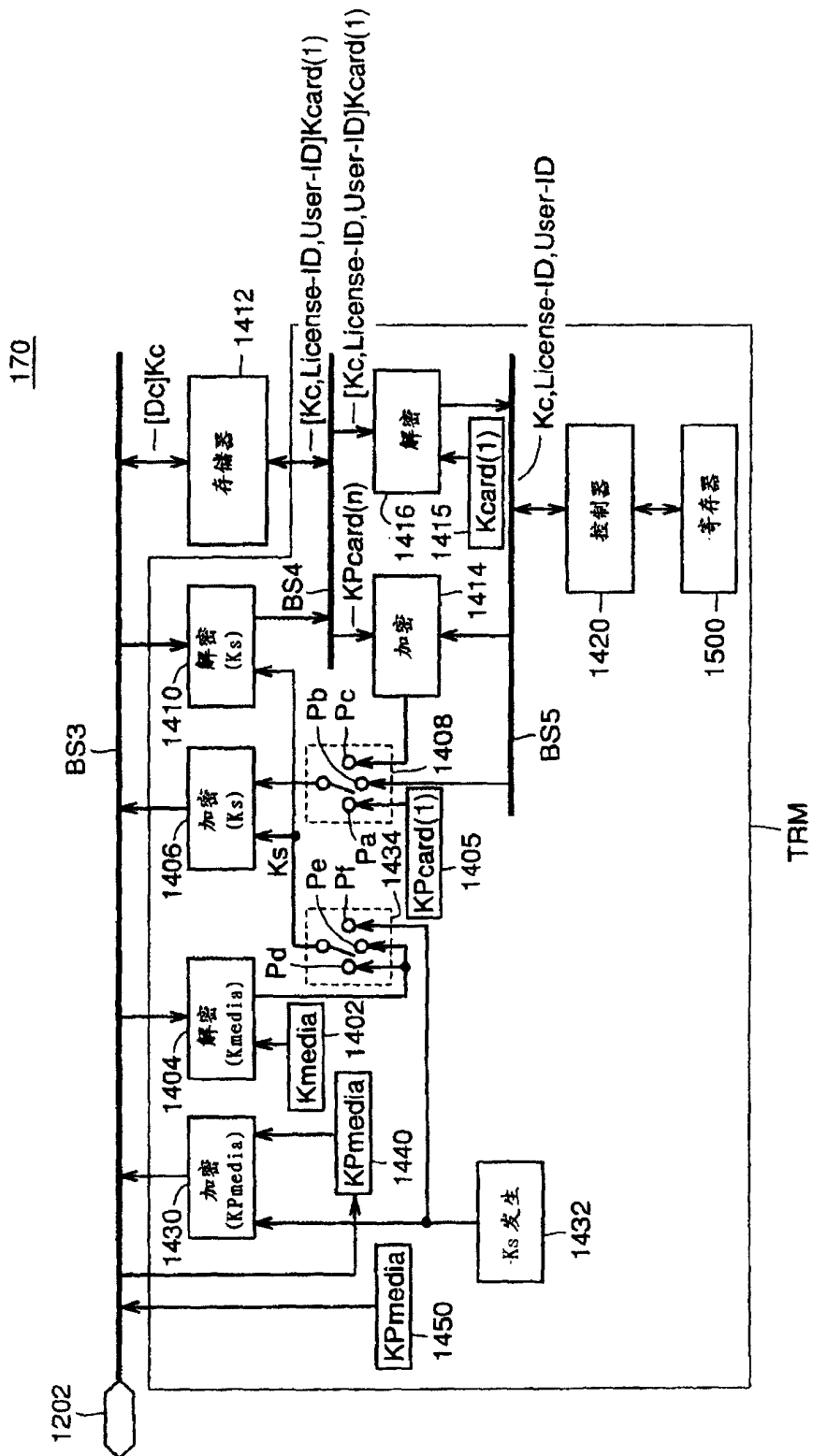


图 22





24

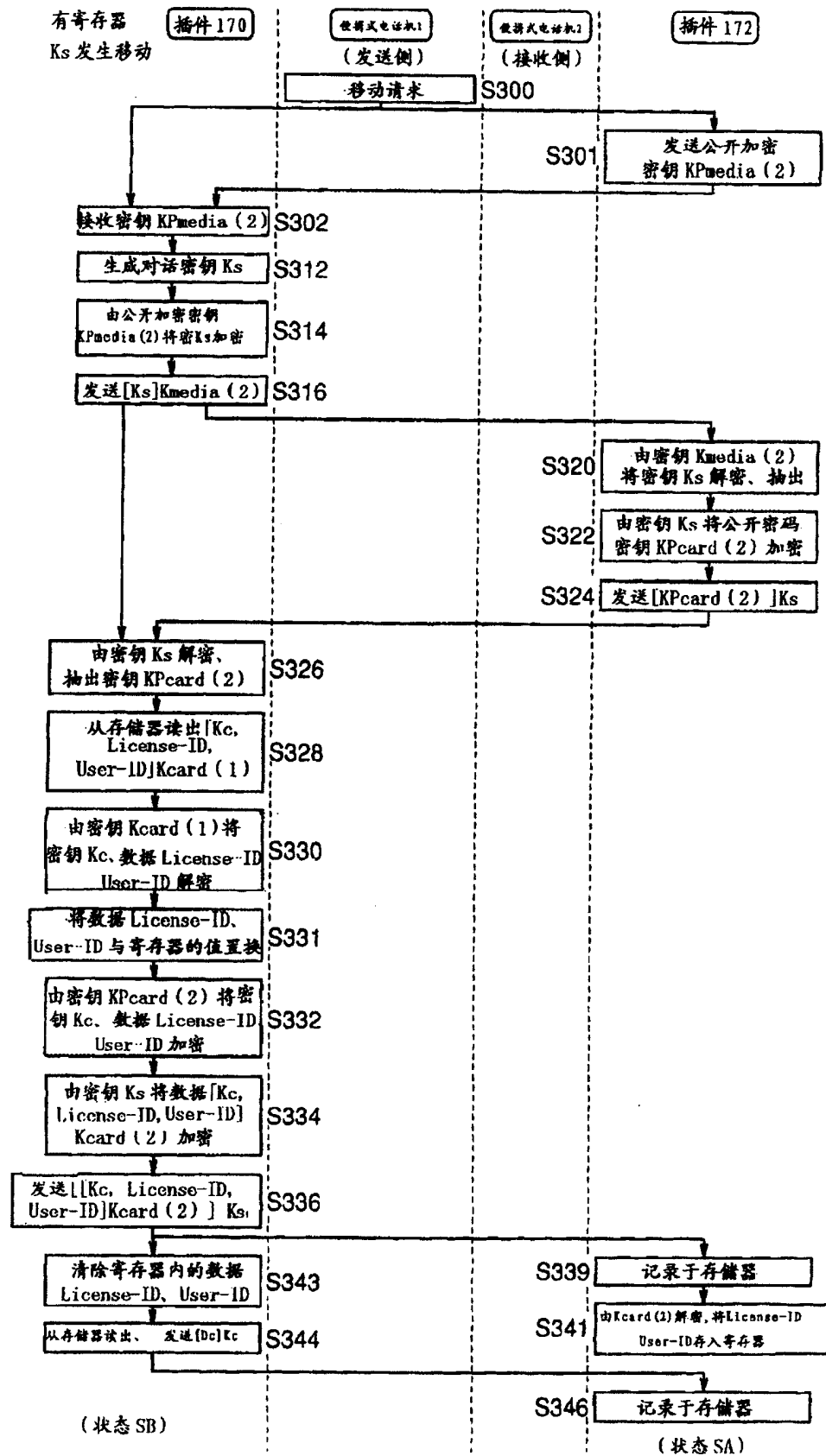


图 25

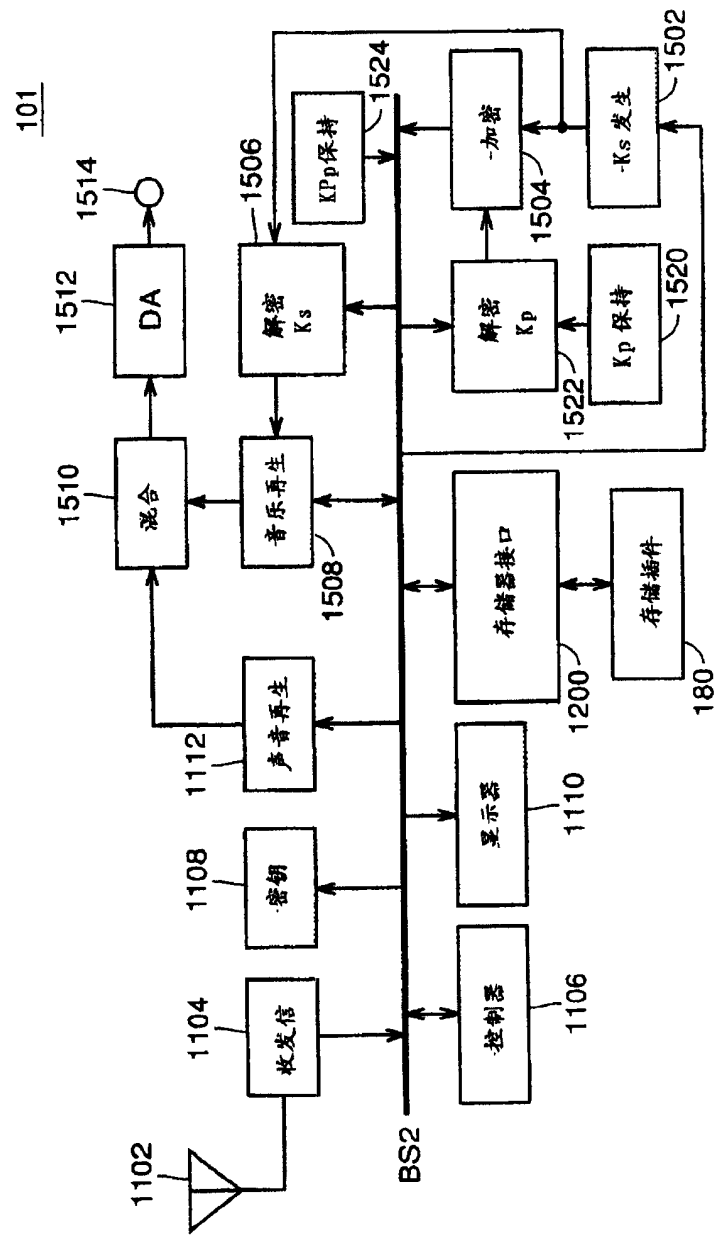


图 26

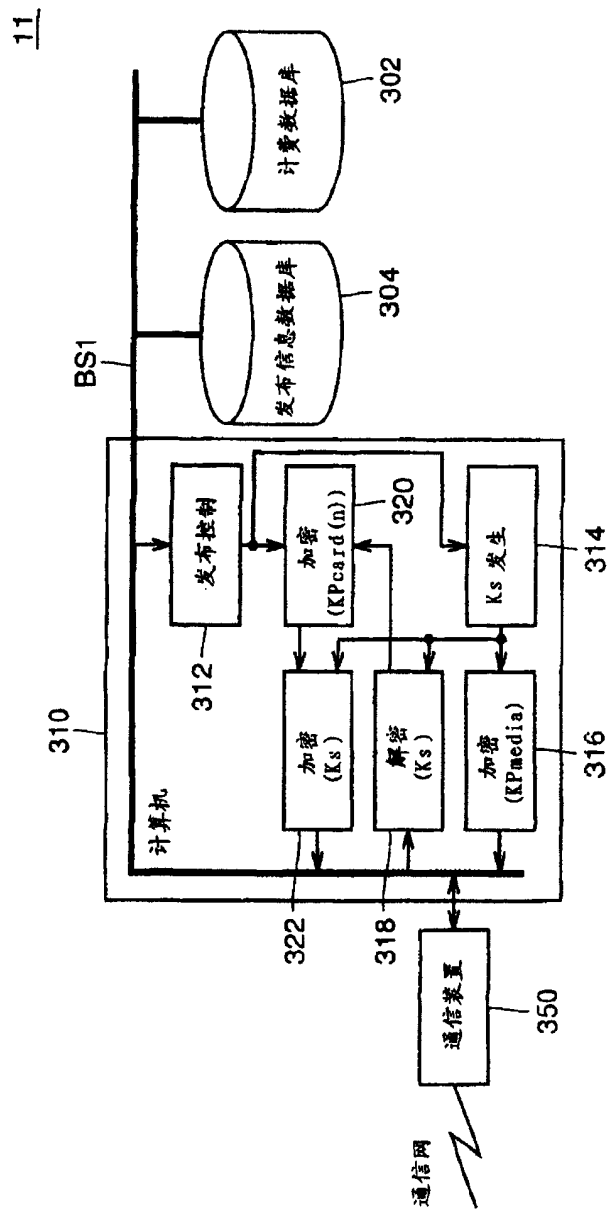


图 27

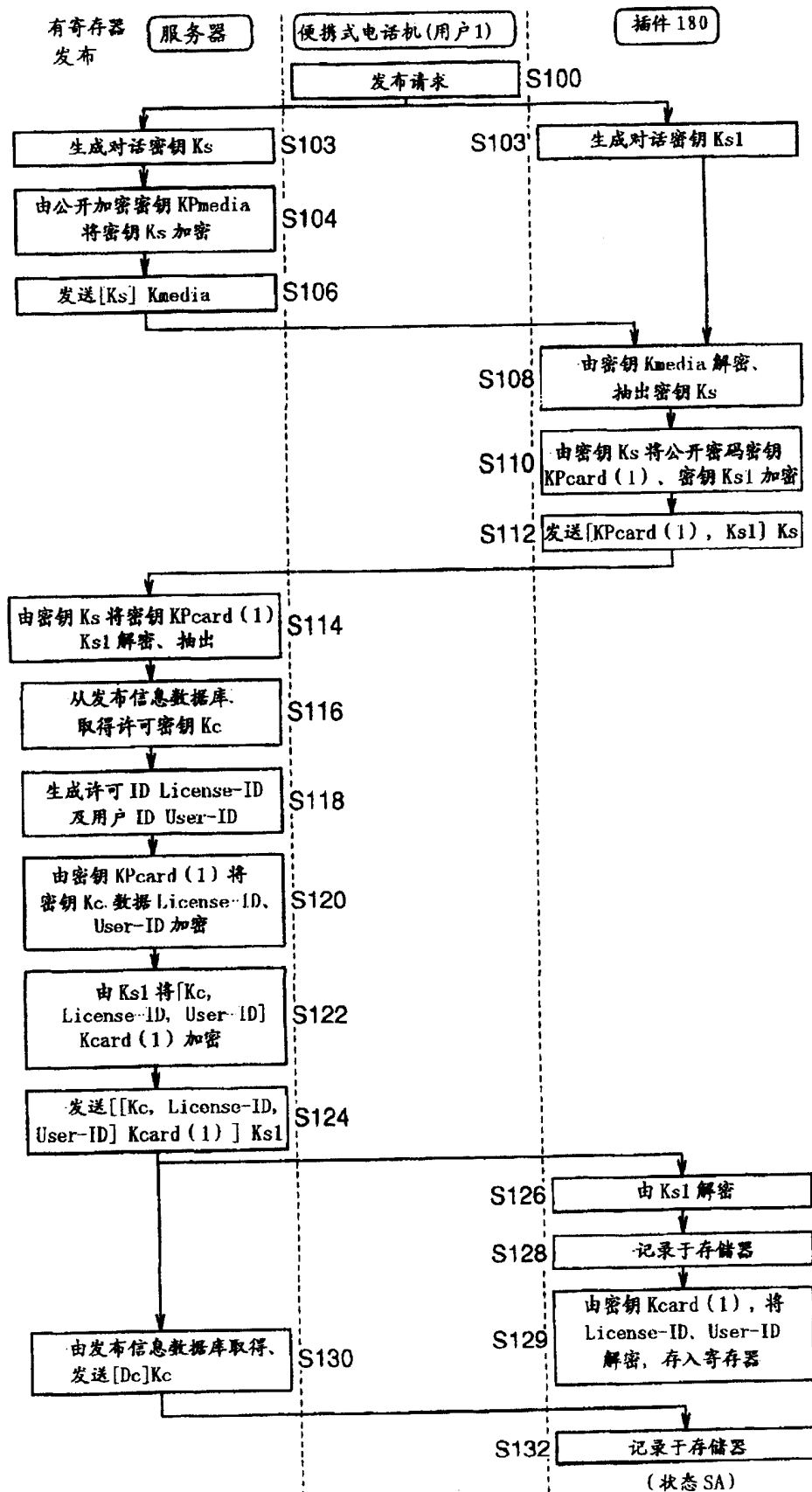


图 29

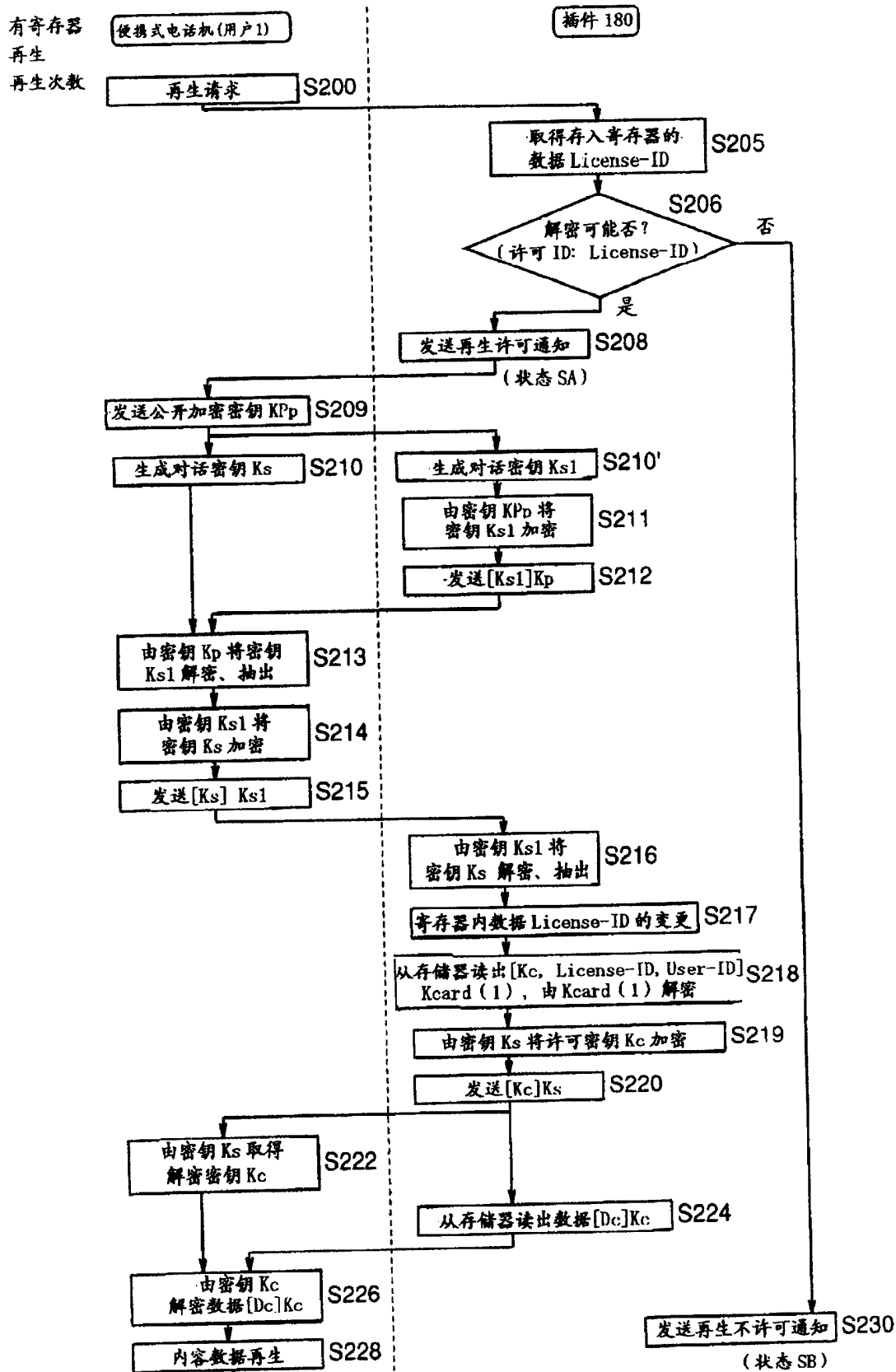


图 30

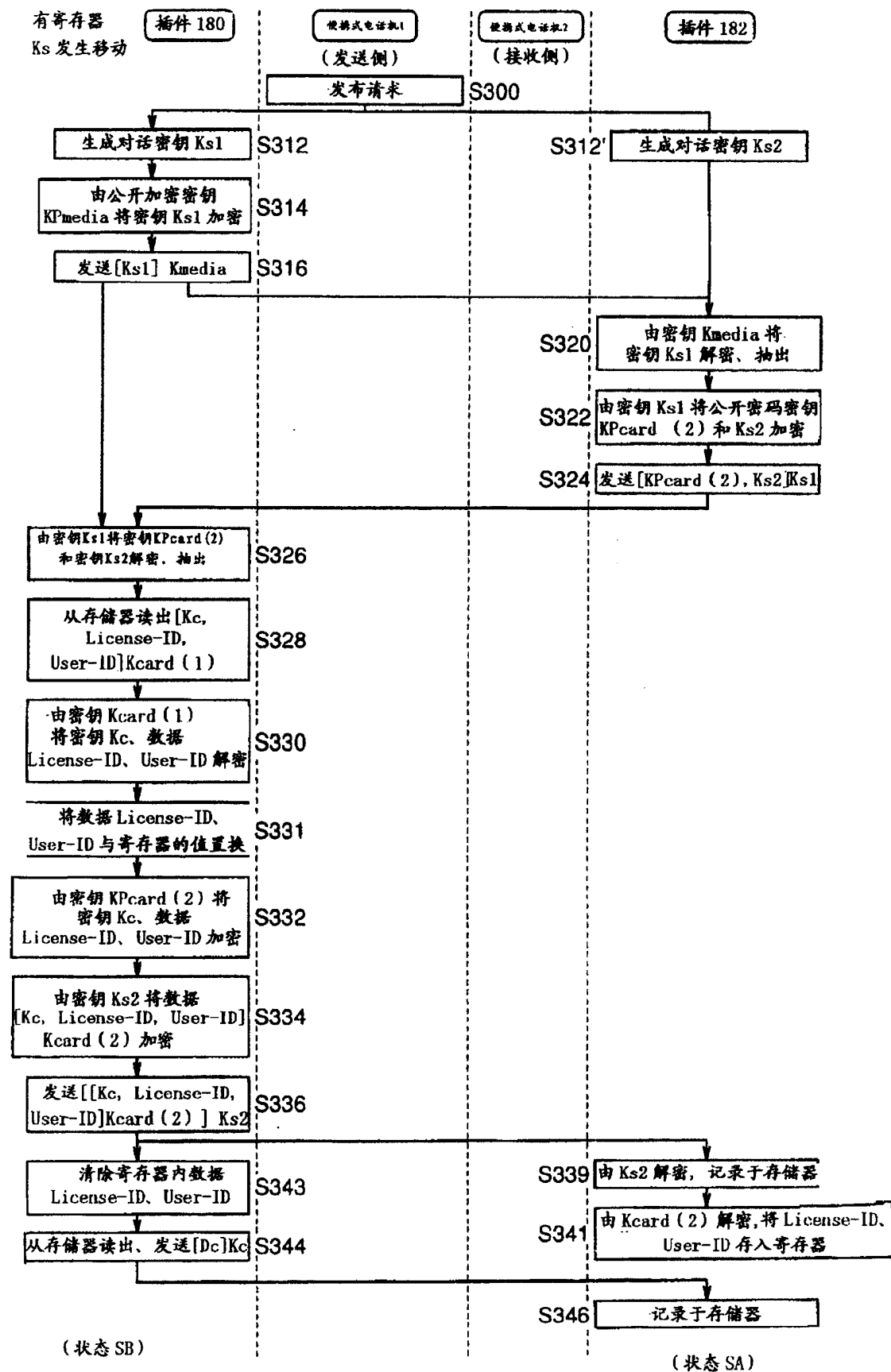


图 31

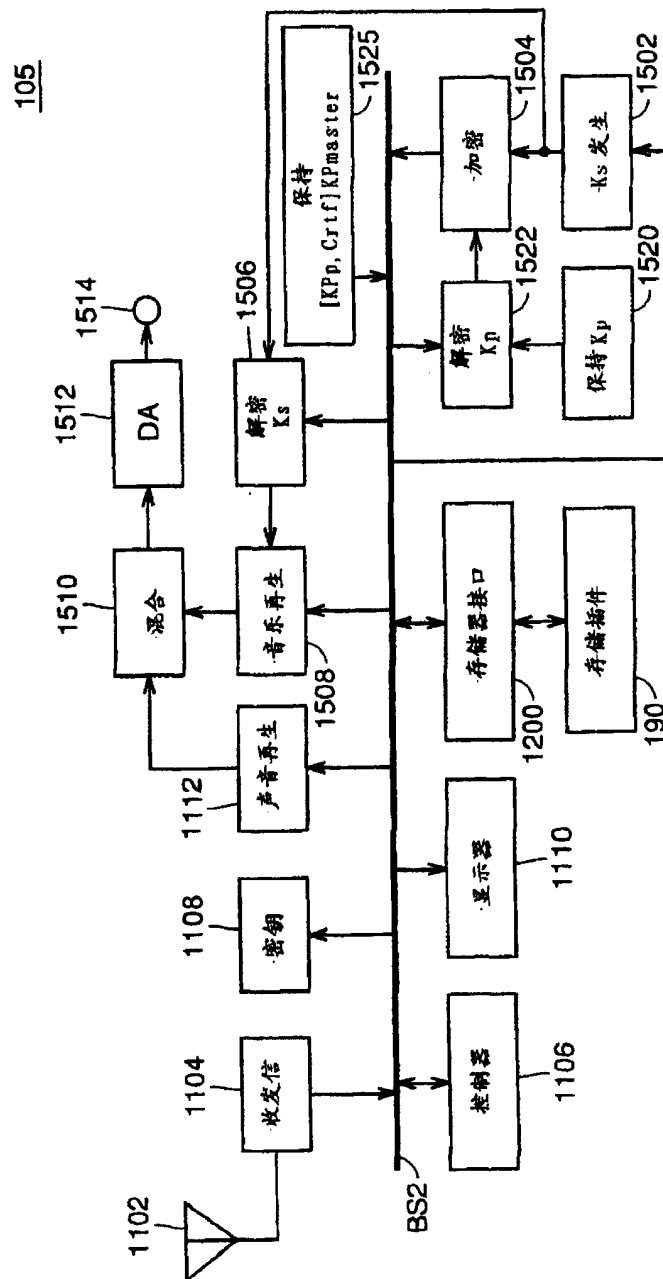


图 32

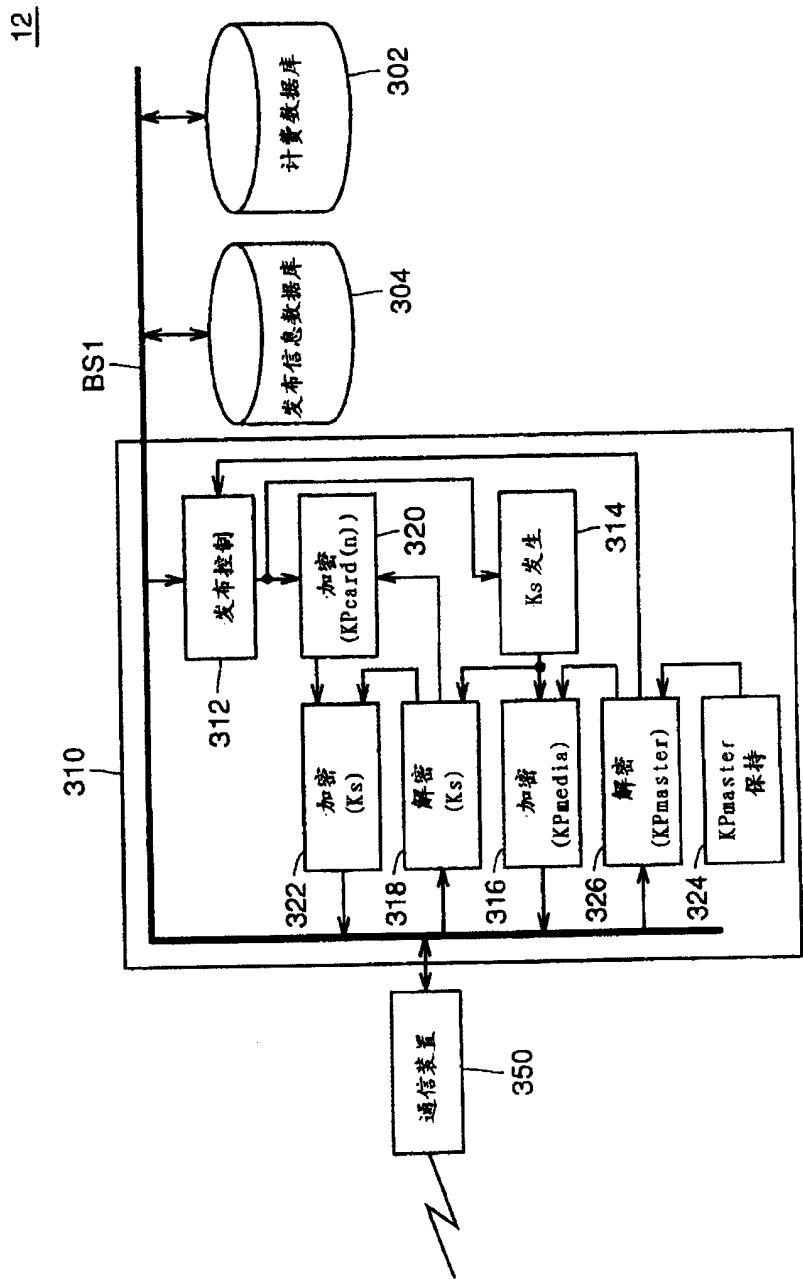


图 33

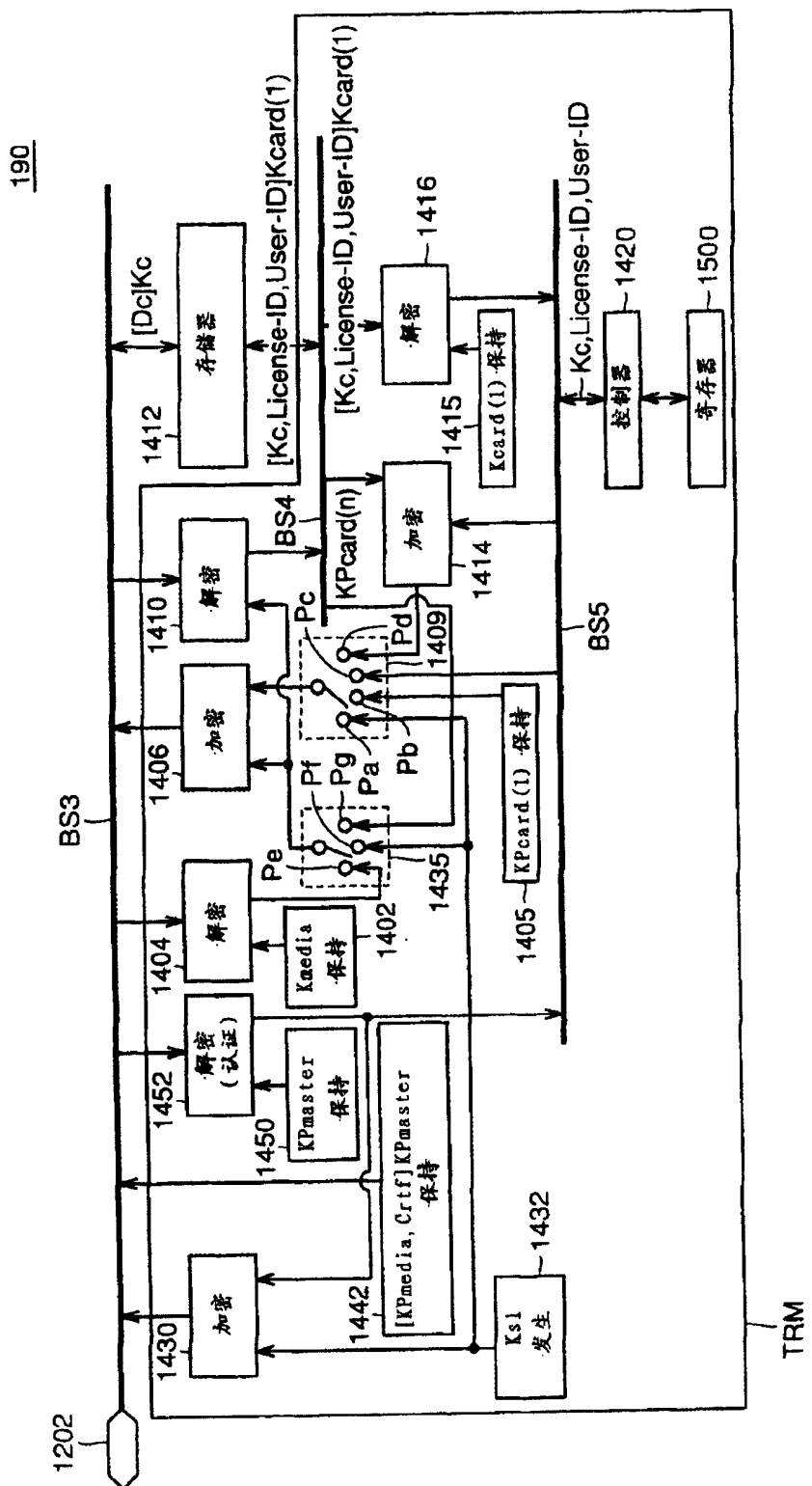


图 34

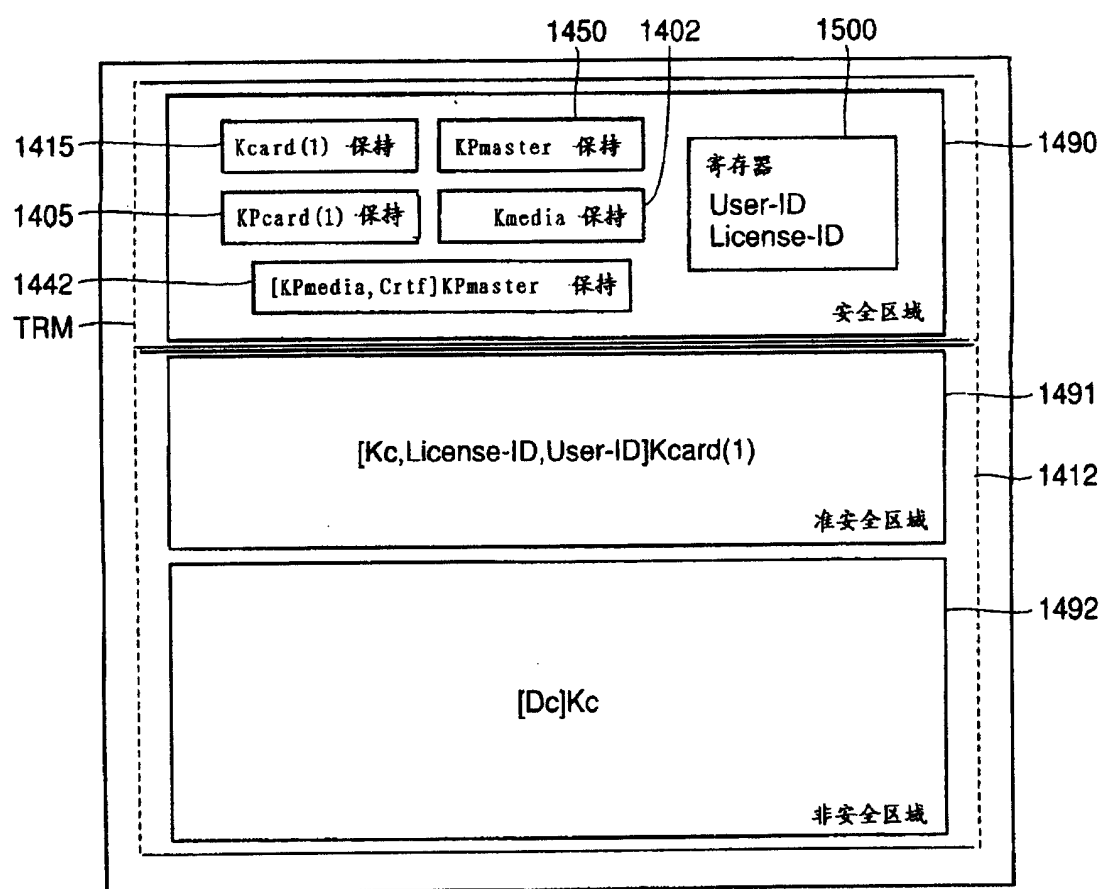


图 35

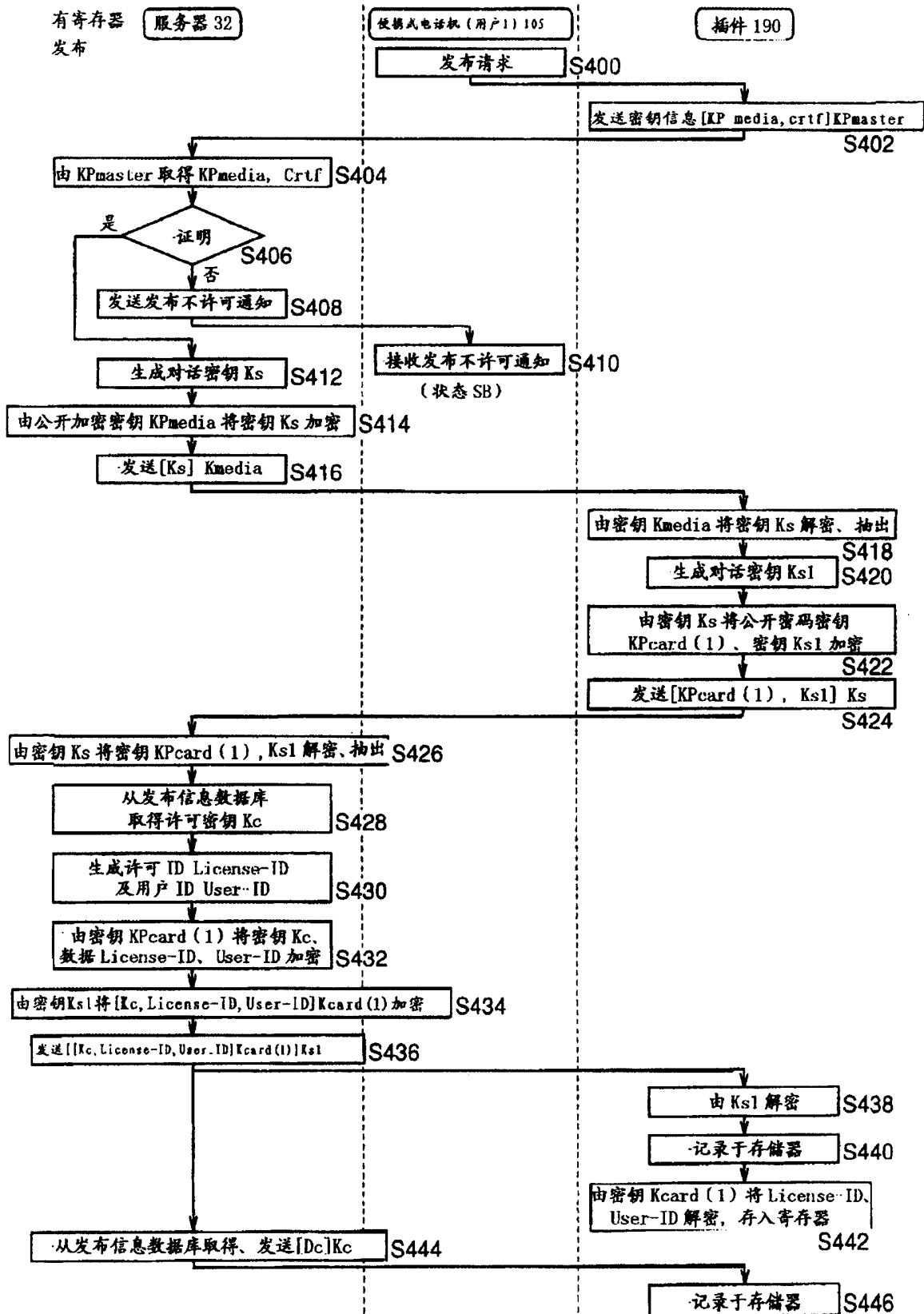


图 36

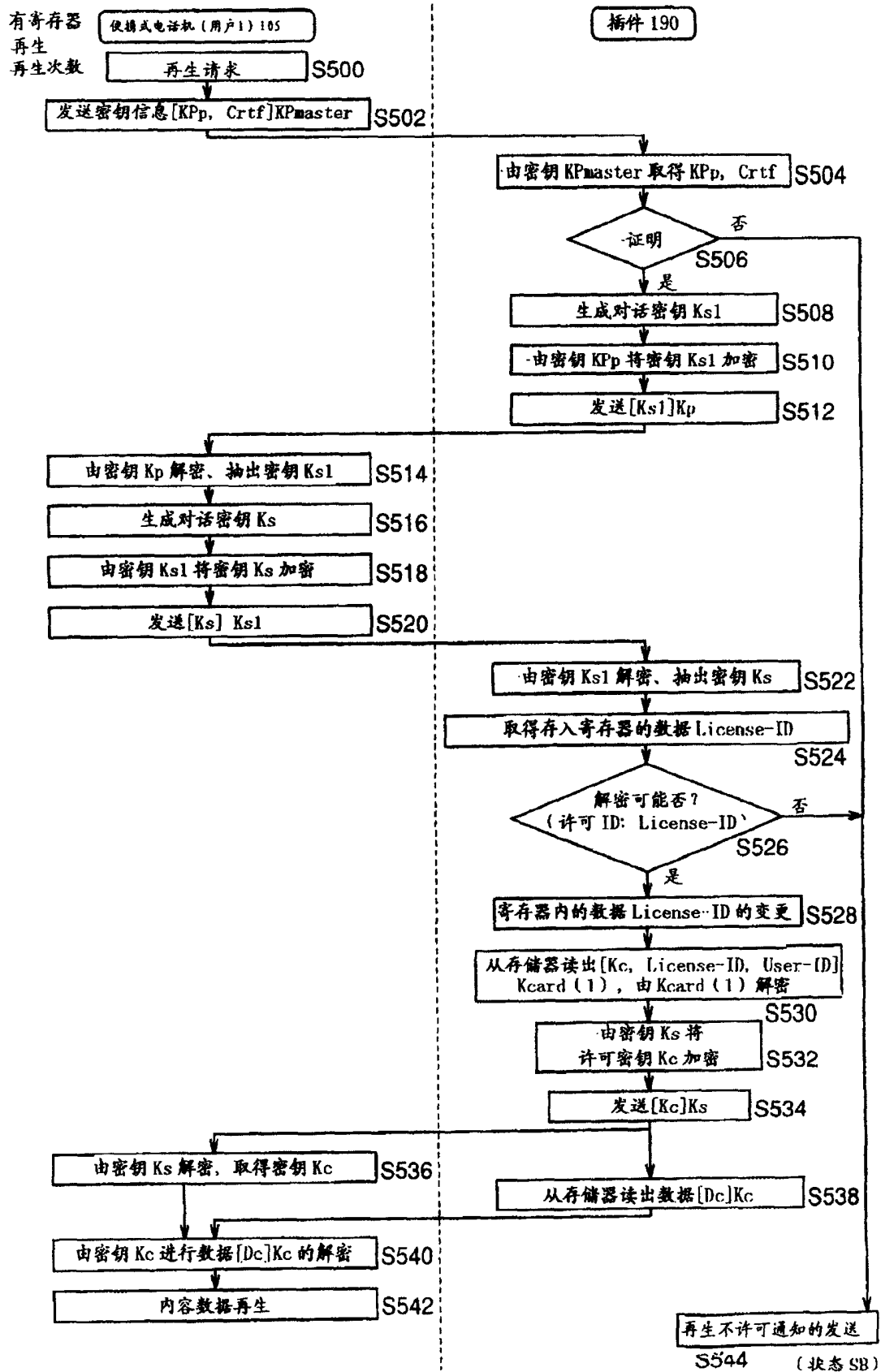


图 37

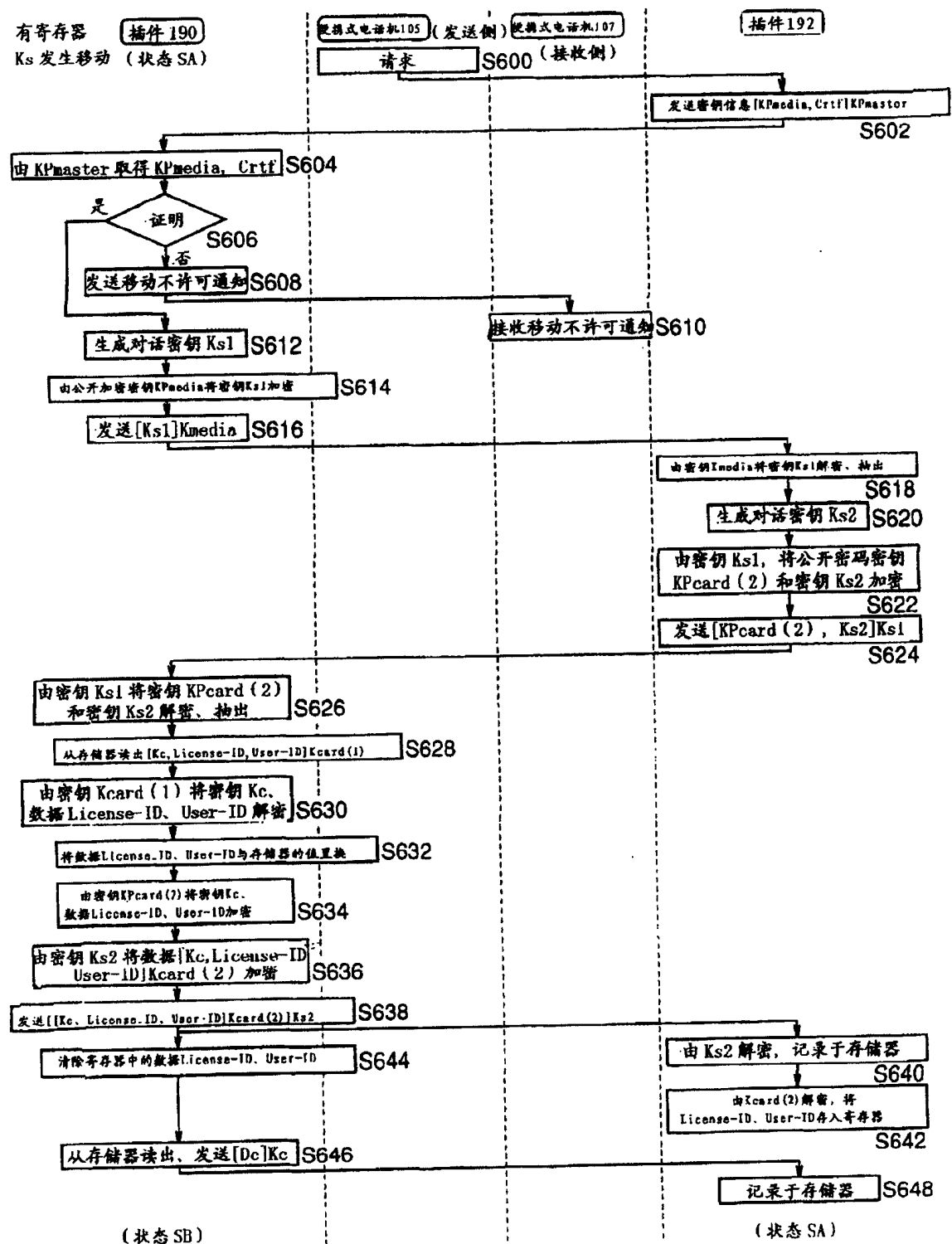


图 38

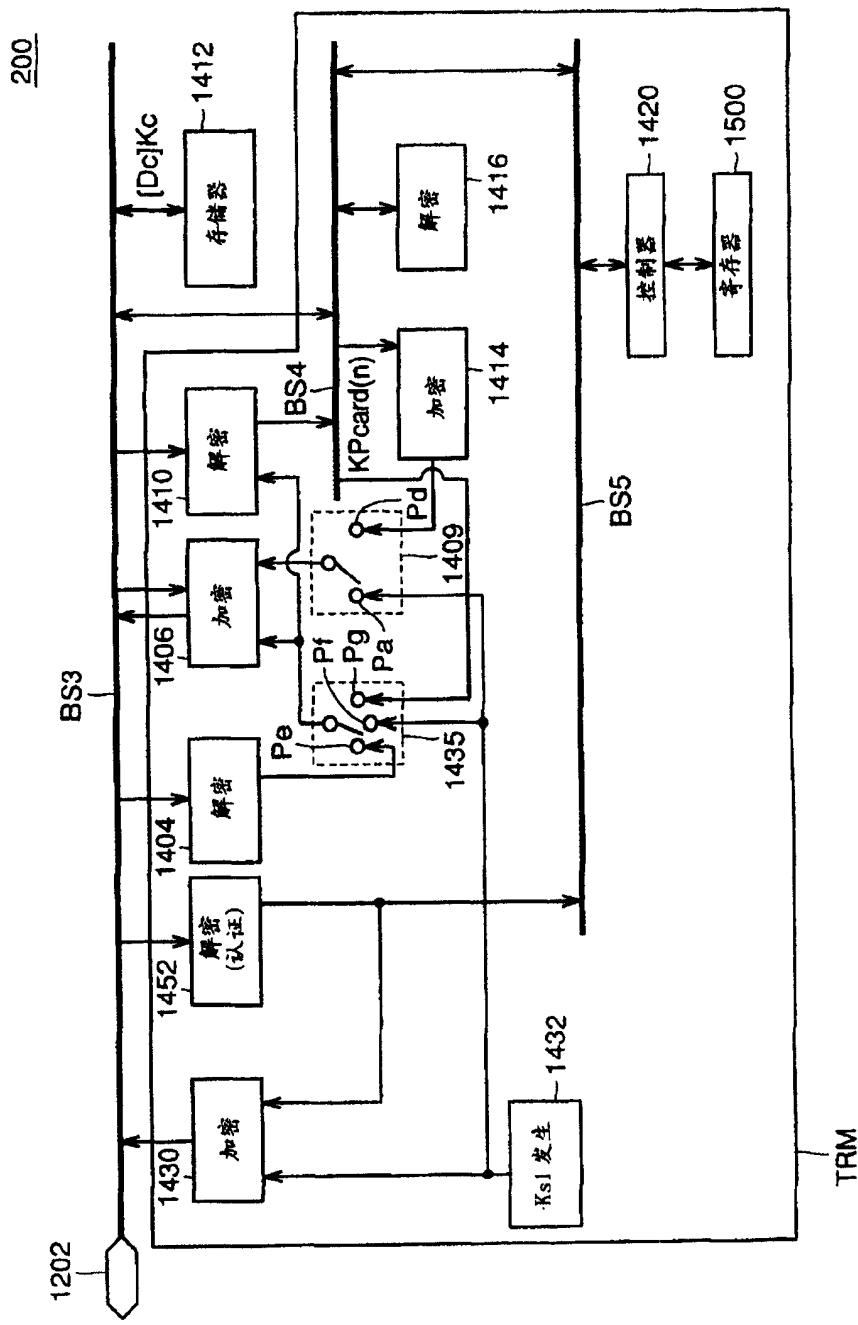


图 39

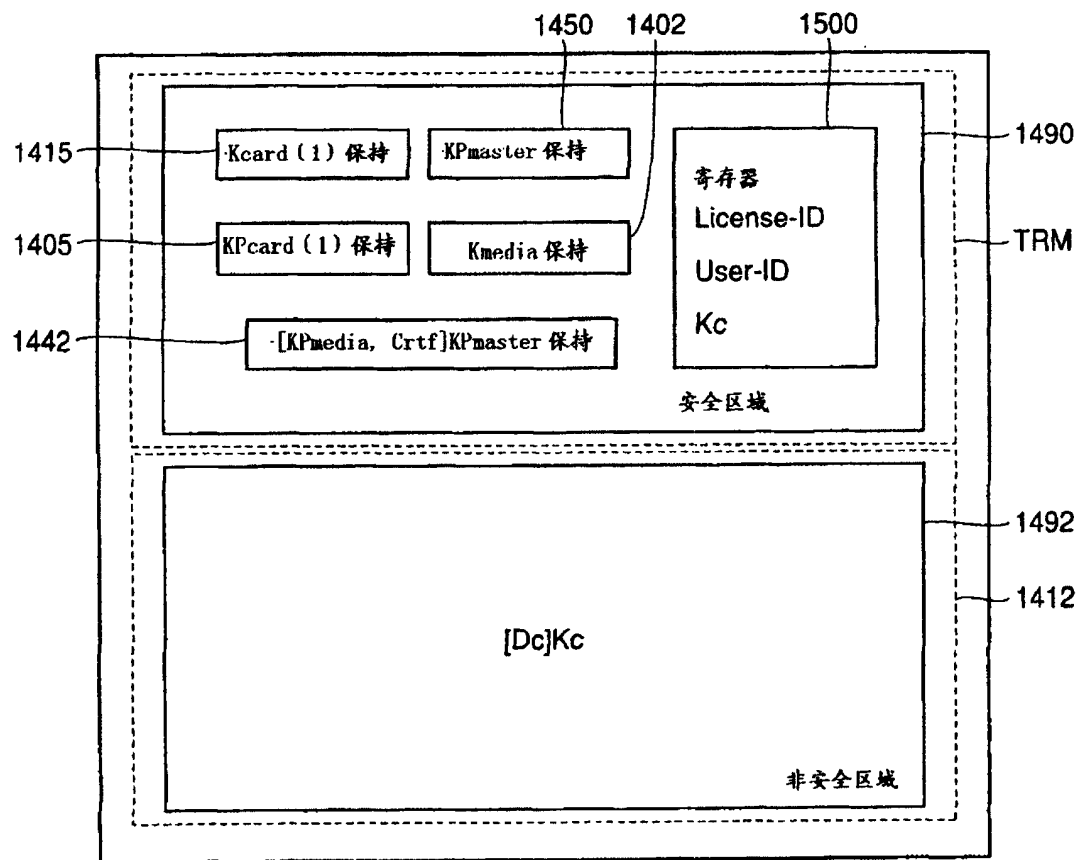


图 40

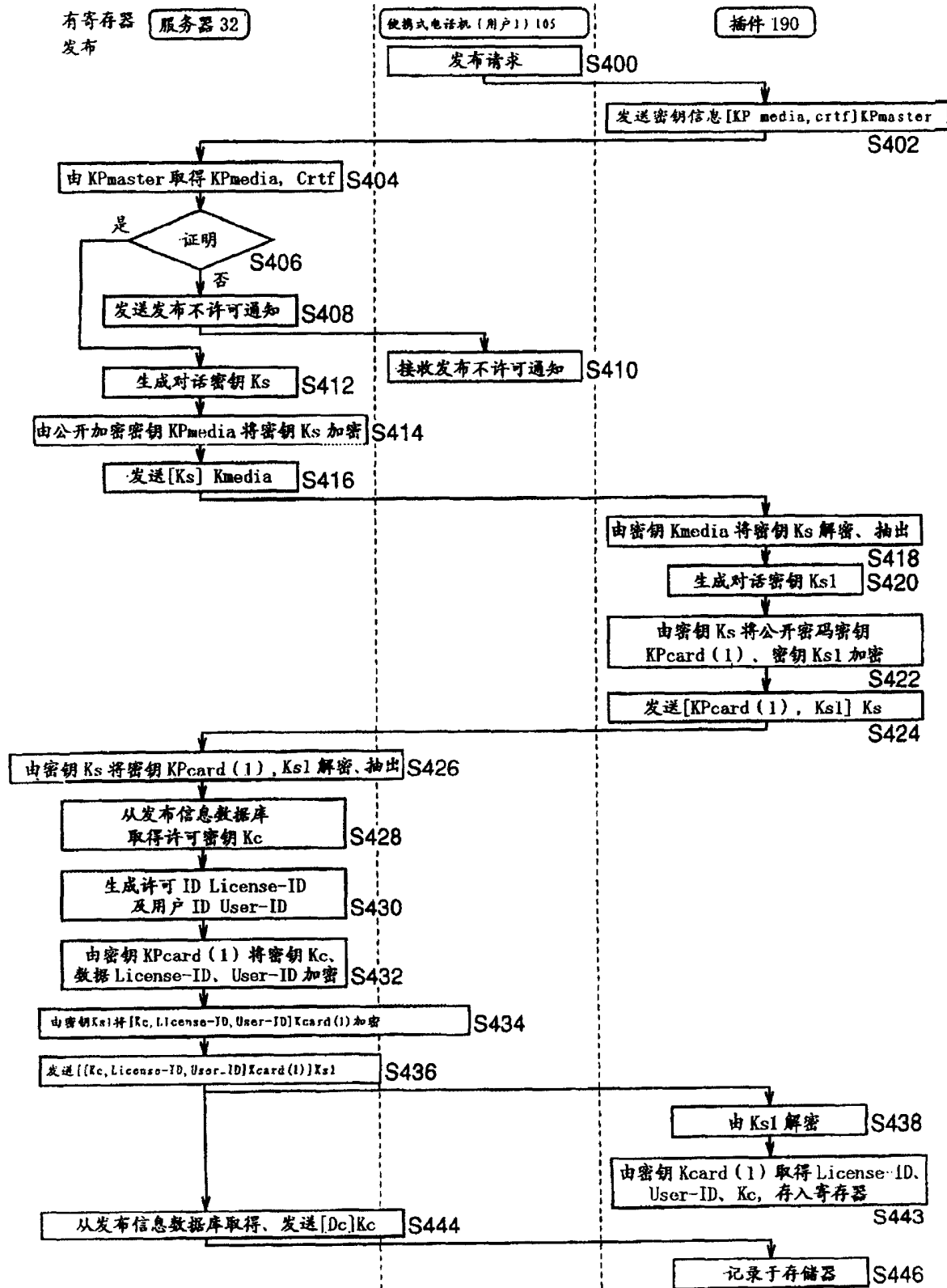


图 41

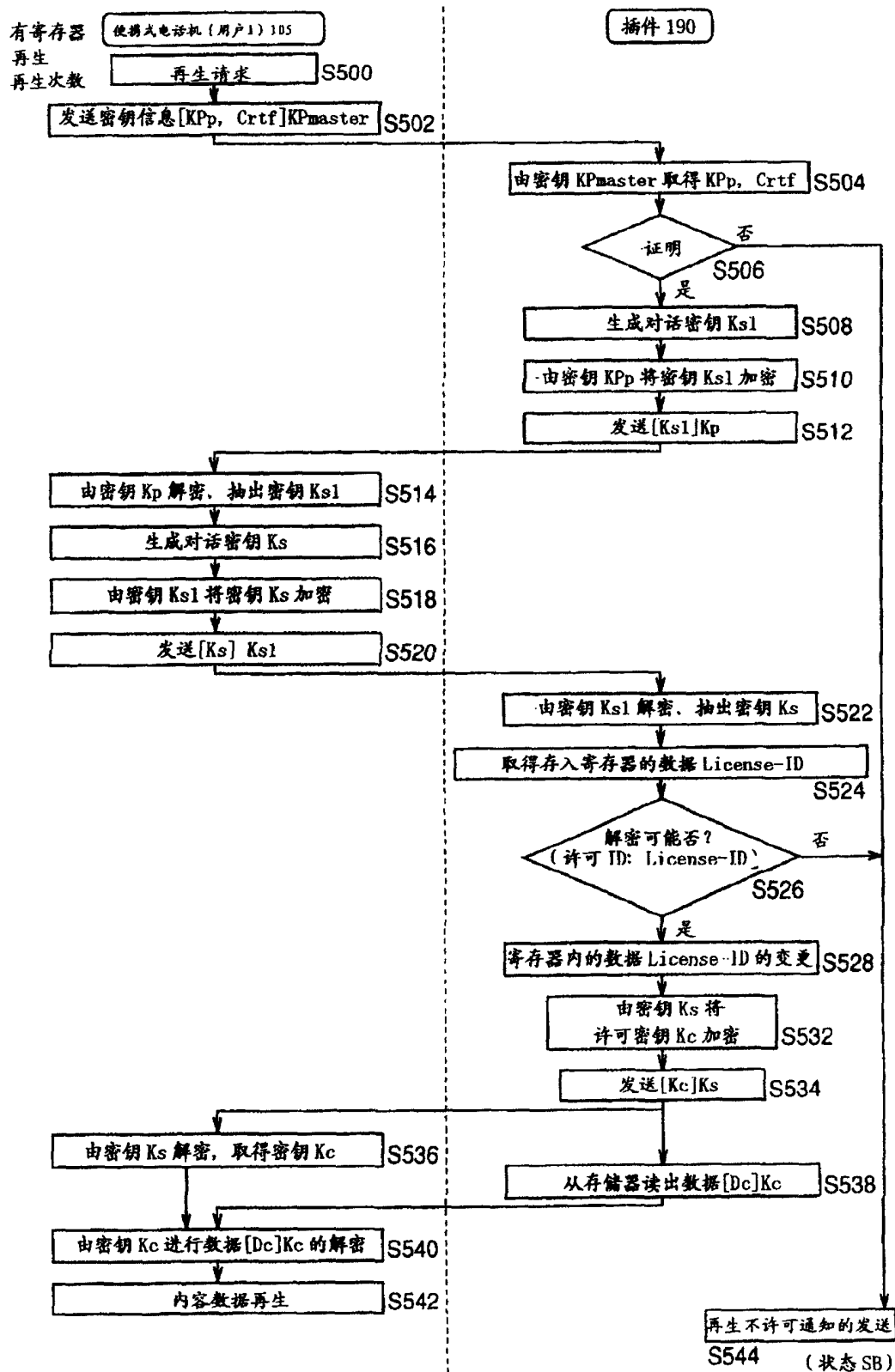


图 42

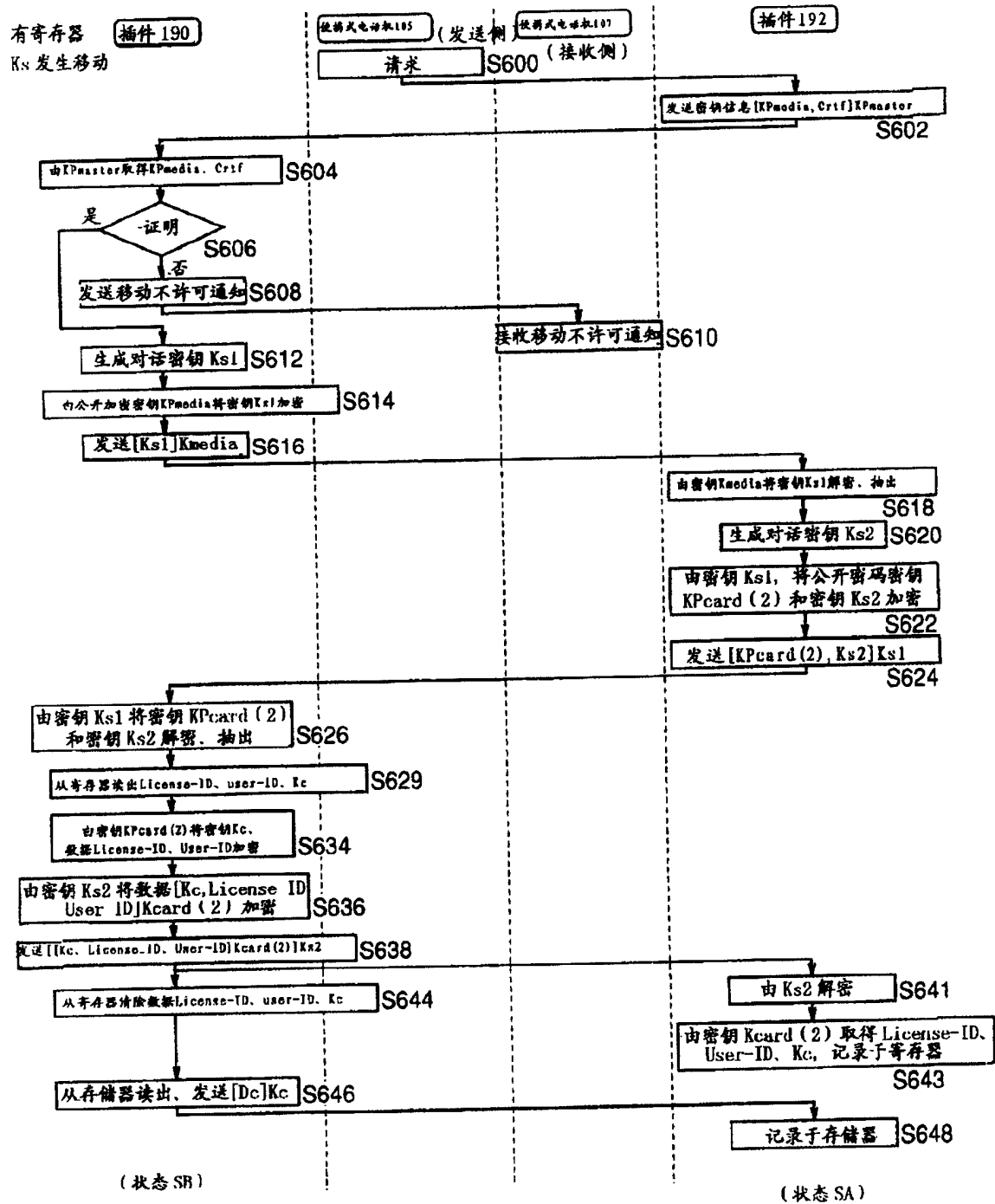


图 43