

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)



[12] 发明专利说明书

专利号 ZL 99111488.4

[45] 授权公告日 2006 年 10 月 11 日

[11] 授权公告号 CN 1279457C

[22] 申请日 1999.7.16 [21] 申请号 99111488.4
[30] 优先权
[32] 1998. 7. 16 [33] JP [31] 201497/98
[71] 专利权人 索尼公司
地址 日本东京都
[72] 发明人 日下部进 高田昌幸 佐佐木将央
审查员 易红春

[74] 专利代理机构 北京市柳沈律师事务所
代理人 马 莹

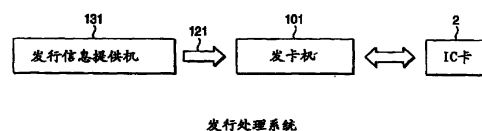
权利要求书 2 页 说明书 43 页 附图 31 页

[54] 发明名称

信息处理装置和信息处理方法

[57] 摘要

在已登录卡的发行信息提供装置 131 中，加密所述已登录卡的发行信息，该加密后的发行信息经传送媒体 121 传送给已登录卡的发卡机 101。在已登录卡的发卡机 101 中，接收和登录来自已登录卡的发行提供装置 131 的加密后的已登录卡的发行信息。当已登录卡的发卡机 101 允许与 IC 卡 2 通信时，它将加密后的已登录卡的发行信息传送给 IC 卡 2。在 IC 卡 2 中，对来自已登录卡的发卡机 101 的加密后的已登录卡的发行信息进行译码，并存储该发行信息。



1. 一种用于向数据存储装置(2)提供管理信息的信息处理装置(131), 所述信息处理装置包括:
- 5 用于形成包含访问数据存储装置的存储区域的密钥的管理信息的形成装置, 所述管理信息包括管理分层结构的存储区域的信息;
- 用于加密管理信息的加密装置, 所述加密装置使用包含在上层管理信息中的密钥, 以加密下层管理信息;
- 用于生成检查码以检查管理信息是否已经被篡改的装置;
- 10 其中所述加密装置将检查码和管理信息一起进行加密; 并且
- 其中所述加密的管理信息被传送到数据存储装置, 以便在数据存储装置中对加密的管理信息进行解密。
2. 根据权利要求1所述的信息处理装置, 其中所述形成装置被配置来形成管理信息, 以至于管理信息包含存储区域识别码, 该识别码能够被分
- 15 配给被管理的存储区域, 并用来识别所述存储区域。
3. 根据权利要求1所述的信息处理装置, 其中所述形成装置被配置来形成管理信息, 以至于管理信息包含关于被管理存储区域的空白容量的信息。
4. 一种数据存储装置(2), 包括:
- 20 数据存储装置, 用于存储数据以提供预定服务, 其中由密钥提供对所述数据存储装置的存储区域的访问;
- 接收装置(53), 用于从外部设备接收加密的管理信息, 其中存储区域以分层结构用管理信息进行管理, 包含有密钥;
- 解密装置(92), 用于使用所述包含在上层管理信息中的密钥对加密的
- 25 管理信息进行解密; 和
- 操作装置, 用于操作检查码以检查管理信息是否已经被篡改; 并且
- 其中所述解密装置对检查码和管理信息一起进行解密。
5. 根据权利要求4所述的数据存储装置, 其中所述接收装置被安排在接触或不接触状态下执行与外部设备的通信。
- 30 6. 根据权利要求4所述的数据存储装置, 其中所述管理信息包含存储区域识别码, 该识别码能够被分配给被管理的存储区域, 并用来识别所述

存储区域。

7. 根据权利要求4所述的数据存储装置，其中所述管理信息包含关于被管理存储区域的空白容量的信息。

8. 一种信息处理方法，包括步骤：

5 形成用于管理分层结构的数据存储设备中的存储区域的管理信息；

 加密管理信息，其中所述加密使用了包含在上层管理信息中的密钥来加密下层管理信息；

 生成检查码以检查管理信息是否已经被篡改的装置；

 传送所述加密的管理信息到数据存储装置；

10 其中所述加密将检查码和管理信息一起进行加密。

信息处理装置和信息处理方法

5 技术领域

本发明涉及一种信息处理装置和一种信息处理方法，并且涉及例如在不回收 IC 卡(集成电路)的情况下能够安全地添加和改变管理信息以便管理包含在所述 IC 卡中的一个存储器的一种信息处理装置和信息处理方法。

10 背景技术

例如，现在已经研制出了希望被用于电子货币系统、安全系统等系统中的 IC 卡(智能卡)。所述 IC 卡具有一个用于执行各种处理的 CPU 和一个用于存储执行所述处理所必要的数据的存储器，在将它电连接到一个预定的读/写器(R/W)或在非接触状态下使用电磁波的同时，执行向/从所述 IC 卡的数据传送/接收。在非接触状态下使用电磁波利用 R/W 执行数据传送/接收的 IC 卡通常被经过电磁波提供电能。

在所述 IC 卡被用于所述电子货币系统、安全系统等等的情况下，数据的安全和诸如防止伪造等安全措施是非常重要的。通常，利用从系统管理者(操作者)给出的一个密钥允许对一个 IC 卡进行访问。即，不具有密钥的个人对 IC 卡的访问受到限制。

另外，在 ISO(国际标准化组织)7816 中规定了所述安全措施，ISO 7816 规定了接触形 IC 卡的标准，根据这个标准，通过锁定与一个引向器(director)或文件夹对应的 DF(专用文件)，限制对与一个文件对应的属于所述 DF 或 EF(基本文件(Elementary File))的层的 DF 进行访问。

通常，所述 IC 卡的管理者或制造者可以回收已经发行给使用者、并在市场上分布的 IC 卡，向每个 IC 卡新添加一文件的所谓卡发行工作，通常是由他们在高度执行所述安全措施的设备等中执行的，对于该文件其中保持有用于提供新服务或用于改变数据访问所需密钥的数据。

即，通常，IC 卡的发行者执行图 1 所示的初始发行工作和向已登录的发行已登录卡发行工作的卡发行经营者发行没有任何功能的 IC 卡(不能执行数据读/写操作的 IC 卡)。已登录卡发行经营者执行已登录的发行工作(二

次(secondary)发行工作), 这样, 希望通过所述 IC 卡发行服务的管理者 #1 能够使用所述 IC 卡。即, 已登录卡的发行者在每个 IC 卡中保持一个将被所述管理者 #1 使用的存储区域(所述管理者 #1 的区域), 并将访问该存储区域所需的密钥和其它信息写入到每个 IC 卡中。这里, 已登录卡发行工作
5 是在诸如所述已登录卡发行经营者的设备等高度执行安全措施的场所(此后称之为“合适和安全场所”)处执行的。另外, 在图 1 中, 所述已登录卡的发行经营者和管理者 #1 经常是同一个人。

经过已登录卡发行工作的 IC 卡被投放到市场并分布给使用者。所述 IC 卡被用于由管理者 #1 提供服务。即, 使用者可以将所述 IC 卡用做电子钥
10 匙或钱包。

当上述已经投放到市场上的 IC 卡是多功能 IC 卡和除管理者 #1 以外的管理者 #2 希望通过所述多功能 IC 卡提供服务时, 已登录卡的发行经营者如图 2 所示暂时收回已经被投放到市场上的 IC 卡。已登录卡的发行经营者执行所述已登录卡发行工作, 从而使管理者 #2 能够使用所述卡。即, 已登
15 录卡的发行经营者在每个 IC 卡中保持一个将被用于管理者 #2 的存储区域(管理者 #2 的区域)并进一步在每个 IC 卡中写入管理者 #2 对所述存储区域进行访问所需的一个密钥和其它信息。此后, 经过了已登录卡的发行工作的所述 IC 卡被再次投放到市场。

例如, 经过已登录卡的发行工作而写入到一个 IC 卡中的密钥是一个对于所述卡的安全性方面非常重要的信息, 并不希望这种信息被分布到诸如
20 市场等的场所, 在这种场所中, 有很大的可能执行诸如分流、篡改等不正常活动, 并且不执行安全性管理(这种场所此后被称之为“不合适和不安全的场所”)。因此, 所述的 IC 卡被从市场回收并如上所述地在一个安全的场所执行已登录卡的发行工作。

25 因此, 每当希望执行所述已登录卡的发行工作时必须回收所述 IC 卡, 这是非常麻烦的。

发明内容

本发明是从这种情况出发进行的, 本发明的一个目的就是使访问一个
30 存储区域所需的密钥和其它信息能够被安全地写入到安全性方面不够安全的场所中。

为了实现上述目的,根据本发明的一个方面,提供了一种信息处理装置,其特征是该装置包括一个加密装置,该装置用于加密包含为管理数据存储装置的一个存储区域而提供的、访问所述数据存储装置的所述存储区域所需的密钥的管理信息。所述加密装置加密包含为管理所述数据存储装置的所述存储区域而提供的、访问所述存储区域所需的密钥的所述管理信息。

根据本发明的另一个方面,提供了一种信息处理方法,其特征是该方法包括一个加密步骤,该步骤用于加密包含有为管理数据存储装置的一个存储区域而提供的、访问所述数据存储装置的所述存储区域所需的密钥的管理信息。包含为管理所述数据存储装置的所述存储区域而提供的、访问所述存储区域所需的密钥的管理信息被加密。

根据本发明的再一个方面,提供了一种信息处理装置,其特征是该装置包括一个译码装置,该装置用于译码包含为管理数据存储装置的一个存储区域而提供的、访问所述数据存储装置的所述存储区域所需的密钥的加密后的管理信息。所述译码装置译码包含为管理所述数据存储装置的所述存储区域而提供的、访问所述存储区域所需的密钥的加密后的管理信息。

根据本发明的再一个方面,提供了一种信息处理方法。其特征是该方法包括一个译码步骤,该步骤用于译码包含为管理数据存储装置的一个存储区域而提供的、访问所述数据存储装置的所述存储区域所需的密钥的加密后的管理信息。包含为管理所述数据存储装置的所述存储区域的、访问所述存储区域所需的密钥的加密后的管理信息被译码。

附图说明

- 图 1 示出了传统 IC 卡的分布图;
- 图 2 示出了传统 IC 卡的分布图;
- 图 3 的框图示出了使用应用了本发明的 IC 卡的卡系统的实施例结构;
- 图 4 的框图示出了图 3 所示读/写器 1 的结构;
- 图 5 的框图示出了图 3 所示 IC 卡 2 的结构;
- 图 6 示出了图 5 所示 EEPROM 66 的逻辑形式的图;
- 图 7 示出了图 5 所示 EEPROM 的目录结构的图;
- 图 8 示出了构成图 7 所示层结构的处理图;

- 图 9 的流程示出了区域形成处理;
- 图 10 的流程示出了服务形成处理;
- 图 11 示出了在多个管理者之间的密钥的接收和传送图;
- 图 12 示出了当管理者 A 提供服务时所需的信息的图;
- 5 图 13 示出了当管理者 A 提供服务时 IC 卡 2 的处理图;
- 图 14 示出了利用服务提供装置 111 执行的所述 IC 卡 2 的确认方法的图;
- 图 15 示出了利用所述 IC 卡 2 执行的服务提供装置 111 的确认方法的图;
- 10 图 16 示出了当管理者 B2 提供服务时所需的信息的图;
- 图 17 示出了当管理者 B2 提供服务时 IC 卡 2 的处理的图;
- 图 18 示出了当管理者 C 提供服务时所需的信息的图;
- 图 19 示出了当管理者 C 提供服务时 IC 卡 2 的处理图;
- 图 20 示出了当管理者 C 提供服务时所需的信息的图;
- 15 图 21 示出了当管理者 C 提供服务时 IC 卡 2 的处理图;
- 图 22 示出了产生用于相互确认的第一访问密钥和第二访问密钥的方法图;
- 图 23 示出了 EEPROM 66 的层结构图;
- 图 24 示出了多个管理者之间的密钥接收/传送的图;
- 20 图 25 示出了多个管理者之间服务(数据)的共同使用的图;
- 图 26 示出了 EEPROM 66 的层结构图;
- 图 27 示出了多个管理者之间密钥的接收/传送图;
- 图 28 示出了本发明的原理图;
- 图 29 的框图示出了应用本发明的已登录卡的发行系统的一个实施例结
- 25 构;
- 图 30 的流程示出了已登录卡的发行信息的提供处理;
- 图 31 示出了加密后的已登录卡的发行信息的格式图; 和
- 图 32 流程示出了译码处理。

30 具体实施方式

下面参考附图描述本发明的最佳实施例。在描述最佳实施例之前, 首

先通过将一个相应的实施例(但是,一个例子)加到在每个装置后面的圆括弧之中以便阐明在“专利权利要求范围”中描述的本发明各装置和随后实施例之间的相应关系来描述本发明的特性。

- 即,本发明第一方面的信息处理装置是一个用于执行处理以便向数据
- 5 存储装置提供管理信息的信息处理装置,该装置包含用于存储数据的数据存储装置(例如,图5所示的EEPROM 66等)、用于存储包含为管理数据存储装置的一个存储区域而提供的、访问所述数据存储装置的所述存储区域所需的密钥的管理信息的管理信息存储装置(例如图5所示的EEPROM 66等)、用于管理所述数据存储装置的管理装置(例如图5所示的定序器91等),
- 10 并且它被提供有一个用于形成所述管理信息的形成装置(例如,图30所示程序的处理步

骤 S21 等)和一个用于加密所述管理信息的加密装置(例如,图 30 所示程序的处理步骤 S23 等)。

上述信息处理装置还包括一个用于运行一个检查码以检查所述管理信息是否被篡改的运行装置(例如,图 30 所示程序的处理步骤 S22 等)和一个用于加密所述检查码以及所述管理信息的加密装置。

上述信息处理装置还包括一个用于经过一个预定传送介质向数据存储装置传送加密后的管理信息的传送装置(例如,图 30 所示程序的处理步骤 S24 等)。

本发明第三方面的信息处理装置是一个具有用于存储数据的数据存储装置(例如,图 5 所示的 EEPROM 等)、用于存储包含为管理所述数据存储装置的所述存储区域而提供的、访问所述数据存储装置的所述存储区域所需的一个密钥的管理信息的管理信息存储装置(例如,图 5 所示的 EEPROM 66 等)和用于管理所述数据存储装置的管理装置(例如,图 5 所述的定序器 91 等)的信息处理装置,和它包括一个用于接收加密后管理信息的接收装置(例如,图 5 所示接口单元 61 等)、用于译码加密后管理信息的译码装置(例如,图 32 所示程序的处理步骤 S32)以及用于将所述管理信息存储到所述管理信息存储装置中的存储控制装置(例如,图 9 所示程序的处理步骤 S4、图 10 所示程序的处理步骤 S14 等)。

所述信息处理装置还包括一个用于检查所述管理信息是否被篡改的检查装置(例如,图 32 所示程序的处理步骤 S33 等)。

不用说,上面的描述并不意味着所述装置被局限于前面所描述的装置。

图 3 示出了使用了应用本发明的 IC 卡的非接触卡系统的实施例的结构(所述系统意味着多个装置的逻辑组合,它不取决于是否在同一个壳体内安置了各自的装置)。

所述非接触卡系统包括 R/W1、IC 卡 2 和控制器 3,使用电磁波在非接触状态下在所述 R/W1 和 IC 卡 2 之间执行数据的传送和接收。

即, R/W1 向 IC 卡 2 传送一个预定的命令, IC 卡 2 接收所述命令并执行与该命令相应的处理。IC 卡 2 向 R/W1 传送与处理结果相应的应答数据。

R/W1 经过一个预定的接口(该接口符合 RS-485A 标准或类似标准)被连接到控制器 3 上,控制器 3 向 R/W1 提供一个预定的控制信号,从而使 R/W1 执行预定的处理。

图4示出了图3所示R/W1的结构。

在IC 21中,用于执行数据处理的DPU(数据处理单元)31、用于处理将被传送给所述IC卡2的数据和从所述IC卡2接收的数据的SPU(信号处理单元)32、与控制器3进行通信的SCC(串行通信控制器)33以及包括用于预先
5 存储处理数据所需信息的ROM部分41和用于在处理期间暂存数据的RAM部分42的存储器单元34,它们经过一个总线彼此互连接。

另外,用于存储预定数据的快闪存储器22也被连接到所述总线上。

DPU 31向SPU 32输出一个将被传送给IC卡2的命令,并从SPU 32接收从IC卡2接收的应答数据。

10 在预定的处理(例如,双相移键控)之后,对将被传送给IC卡2的所述命令执行调制(编码成曼彻斯特码等),SPU 32将其输出给调制电路23,并且,它还从解调电路25接收由所述IC卡2传送的应答数据,并对所述数据执行预定的处理。

调制电路23在由SPU 32所提供数据的基础上,对具有由振荡器(OSC)26
15 提供的预定频率(例如,13.56MHz)的载波执行ASK(幅值移位键入)调制,并经过天线27向IC卡2输出作为电磁波而如此产生的调制波。此时,设计所述调制电路23使其调制因数被设置成小于1和执行所述ASK调制,借此,即使是在数据低电平处,也能够避免所述调制波被减小到零。

解调电路25解调经过天线27接收的调制波(经过ASK调制的波),并向
20 SPU 32输出被如此解调的数据。

图5示出了图3所述IC卡2的结构。

在IC卡2中,IC 51接收从R/W1经过天线53传送的调制波。电容器52与天线53一起共同构成了一个LC电路,设计该LC电路,以使其能够利用具有预定频率(载波频率)的电磁波进行调谐(振荡)。

25 在IC 51中,RF接口单元61利用ASK解调器81检测和解调经过天线53接收的调制波(被进行ASK调制的波),并向BPSK解调电路62和PLL(锁相环)单元63输出被如此解调的数据。另外,它利用电压调节器82稳定在ASK解调器81中检测到的信号,并将它作为DC电源提供给每个电路。

在振荡电路83中,RF接口单元61使具有和所述数据的时钟频率相同
30 频率的一个信号振荡,并向PLL单元63输出所述信号。

在RF接口单元61中,用作IC卡2的电源的天线53的负载随同ASK

调制器 81 中从运行单元 64 经过 BPSK 调制电路 68 提供的数据变化(例如, 规定的转换元件随同数据导通/截止, 并且只有当所述转换元件被导通时, 预定的负载才会被并行连接到天线 53 上), 借此, 经过天线 53 接收的所述调制波被进行 ASK 调制(当从 IC 卡 2 传送数据(IC 卡 2 被用于传送数据)时, R/W1 5 将从它输出的所述调制波的最大幅值设置成一个固定值, 和在天线 53 负载变化的基础上这个调制波被进行 ASK 调制), 并经过天线 53 将它的调制分量传送给 R/W1(改变 R/W1 的天线 27 的端电压)。

在从 ASK 解调器 81 提供的数据的基础上, PLL 单元 63 产生一个与所述数据同步的时钟信号, 并将该时钟信号输出给 BPSK 解调电路 62 和 BPSK 10 调制电路 68。

当在 ASK 解调器 81 中解调的数据被进行 BPSK 调制时, BPSK 解调电路 62 根据从 PLL 单元 63 提供的所述时钟信号解调所述数据(译码曼彻斯特码), 并向运行单元 64 输出被如此解调的数据。

当从 BPSK 解调电路 62 提供的数据被加密时, 在加密/译码单元 92 中, 15 运行电路 64 译码所述数据, 然后, 在定序器 91 中处理所述数据。当所述数据没有被加密时, 从 BPSK 解调电路 62 提供的数据被直接提供给定序器 91, 不经过所述加密/译码单元 92。

定序器 91 被设计成执行与作为将被提供给它的命令的数据相对应的处理。即, 例如, 定序器 91 执行向/从 EEPROM 66 的数据写入和读出操作和 20 其它必要的操作处理。另外, 定序器 91 在确认的基础上执行对 EEPROM 66 的访问控制和管理 EEPROM 66。

在存储在 EEPROM 66 中的所述数据的基础上, 运行单元 64 的奇偶运算符 93 计算作为奇偶性的 Reed Solomon 代码。

在定序器 91 中运行单元 64 执行预定的处理之后, 它向 BPSK 调制电路 25 68 输出与所述处理对应的应答数据(将被传送给 R/W1 的数据)。

BPSK 调制电路 68 对从运行单元 64 提供的数据进行 BPSK 调制, 并向 RF 接口单元 61 的 ASK 调制器 84 输出被如此调制的数字。

ROM(只读存储器)65 存储被定序器 91 用于执行它的处理的一个程序和其它必要的数字。RAM 67 暂存定序器 91 处理期间的数字。

30 EEPROM(电可擦和可编程 ROM)66 是一个非易失存储器, 即使是当 IC 卡 2 结束与 R/W1 的通信和电源停止时, 它也将继续存储数字。

下面将描述在 R/W1 和 IC 卡 2 之间的数据传送/接收处理。

R/W1(图 4)从天线 27 发射一个预定的电磁波, 监视天线 27 的负载状态并且等待直到检测到由于 IC 卡 2 的逼近而引起所述负载状态的变化。R/W1 可以执行一个处理(轮询), 在这个处理中, 发射在预定短模式数据的基础上
5 被进行了 ASK 调制的电磁波, 以呼叫 IC 卡 2, 直到在一个固定的时间内获得来自 IC 卡 2 的应答为止。

当在 R/W1 中检测到 IC 卡 2 的逼近时, R/W1 的 SPU 32 把一个预定频率(例如, 是所述数据频率的两倍的频率)的矩形波作为载波, 在将被传送给 IC 卡 2 的数据(与将被 IC 卡 2 执行的处理对应的命令、将被写入到 IC 卡 2
10 的写入数据等)的基础上对所述预定频率的矩形波进行 BPSK 调制, 和向调制电路 23 输出被如此产生的调制波(BPSK 调制信号)(曼彻斯特码)。

在所述 BPSK 调制处理中, 使用微分变换, 所述数据可以和所述调制波的相位变化相互关联, 在这种情况下, 即使是当它被反相时, 所述 BPSK 调制信号也可以被解调成原来的信号。因此, 在解调操作中不需要考虑所
15 述调制波的极性。

在所输入的 BPSK 调制信号的基础上, 调制电路 23 利用小于 1(例如, 0.1)的一个调制因数(= 数据信号的最大幅值/载波的最大幅值)对所述预定载波进行 ASK 调制, 和经过天线 27 向 IC 卡 2 输出被如此产生的调制波(ASK 调制波)。

20 当不执行传送时, 调制电路 23 产生具有例如数字信号两级电平(高电平和低电平)中的高电平的调制波。

在 IC 卡 2(图 5)中, 从 R/W1 的天线 27 发射的部分电磁波在包括天线 53 和电容器 52 的一个 LC 电路中被转换成电信号, 该电信号(调制波)被输出给 IC 51 的 RF 接口 61。RF 接口 61 的 ASK 解调器 81 通过整流和平滑所述调制波检测一个包络并将如此产生的信号提供给电压调节器 82。另外,
25 它抑制所述信号的 DC 分量以提取所述数据信号, 并向 BPSK 解调电路 62 和 PLL 电路 63 输出所述数据信号。

此时, 天线 53 的端电压 V_0 如下:

$$V_0 = V_{10}(1 + K \times V_s(t)) + \cos(\omega t)$$

30 其中, $V_{10}\cos(\omega t)$ 表示载波, K 表示调制因数和 $V_s(t)$ 表示从 SPU 32 输出的数据。

在利用 ASK 解调器 81 进行整流后电压 V_1 的低电平值 V_{LR} 如下：

$$V_{LR} = V_{10}(1 + K \times (-1)) - V_f$$

这里，在 ASK 解调器 81 中， V_f 表示构成用于整流和平滑的整流电路的二极管(未示出)的电压降，通常它大约等于 0.7 伏电压。

5 当接收经过 ASK 解调器 81 整理和平滑的信号时，电压调节器 82 稳定所述信号并将该信号作为 DC 电源提供给各个电路和运行单元 64。在这种情况下，由于如上所述所述调制波的调制因数 K 小于 1，所以，整流后的电压变化(高电平和低电平之间的差)很小。因此，可以在电压调节器 82 中很容易地产生所述 DC 电源。

10 这里，当接收具有 5 % 的调制因数 K 的调制波从而使得 V_{10} 大约是 3 伏电压时，整流后的低电平电压 V_{LR} 等于 $2.15 (= 3 \times (1 - 0.05) - 0.7)$ 伏电压或更多，并且电压调节器 82 能够向每个电路提供足够的电压作为电源。在这种情况下，整流后电压 V_1 的 AC 分量(数据分量)的幅值 $2 \times K \times V_{10}$ (峰-峰值)等于 $0.3 (= 2 \times 0.05 \times 3)$ 伏电压或更多，并且 ASK 解调器 81 能够以足够高的
15 的 S/N 比值对所述数据进行解调。

如上所述，通过使用具有小于 1 的调制因数 K 的 ASK 调制波，可以执行具有低误差率(在高 S/N 比的状态下)的通信，和可以向 IC 卡 2 提供足够作为电源的 DC 电压。

当从 ASK 解调器 81 接收数据信号(BPSK 解调信号)时，BPSK 解调电路
20 62 根据从 PLL 电路 63 提供的时钟信号解调所述数据信号并向运行单元 64 输出被如此解调的数据。

当从 BPSK 解调电路 62 提供的数据被加密时，运行单元 64 在加密/译码单元 92 中译码所述数据，然后将所述数据(命令)提供给定序器 91 以对所述数据进行处理。在这个时间周期期间内，即在从所述数据被传送给 IC 卡 2
25 的时间开始到接收对所述传送的应答时间结束的周期期间内，R/W1 传送其值为 1 的数据并且处于备用状态。因此，在这个时间周期内，IC 卡 2 接收其最大幅值是恒定的调制波。

在所述处理结束之后，定序器 91 向 BPSK 调制电路 68 输出处理结果的数据等(将被传送给 R/W1 的数据)。在 R/W1 的 SPU 32 的情况相同，BPSK
30 调制电路 68 对所述数据进行 BPSK 调制(编码成曼彻斯特码)，并向 RF 接口单元 61 的 ASK 调制器 84 输出调制后的数据。

ASK 调制器 84 使用一个切换元件或类似元件根据来自 BPSK 调制电路 68 的数据改变连接到天线 53 两端的负载,借此,所接收的调制波(如上所述,在传送来自 IC 卡 2 的数据时,从 R/W1 输出的调制波的最大幅值是恒定的)根据将被传送的数据进行 ASK 调制,以改变 R/W1 的天线 27 的端电压,然后,将被如此调制的数据传送给 R/W1。

在接收来自 IC 卡 2 数据的时间处, R/W1 的调制电路 23 持续传送其值为 1(高电平)的数据。在解调电路 25 中,在被电磁耦合到 IC 卡 2 的天线 53 的天线 27 的端电压微小变化(例如,数十微伏)的基础上检测从 IC 卡 2 传送的数据。

另外,在解调电路 25 中,利用一个高增益放大器(未示出)放大和调制被检测到的信号(ASK 调制波),和如此获得的数据被输出给 SPU 32。SPU 32 解调所述数据(BPSK 调制信号),并将其输出给 DPU 31。DPU 31 对来自 SPU 32 的数据进行处理并在所述处理结果的基础上判断所述通信是否应当结束。如果判断的结果是再次执行所述通信,则与上述情况相同,执行 R/W1 和 IC 卡 2 之间的通信。相反,如果判断的结果是结束所述通信,那么, R/W1 结束与 IC 卡 2 的通信处理。

如上所述, R/W1 使用其中所述调制因数 K 小于 1 的 ASK 调制向 IC 卡 2 传送数据, IC 卡 2 接收所述数据以执行与所述数据对应的处理并将与所述处理结果对应的数据返回给 R/W1。

图 6 示出了图 5 所示 EEPROM 66 的逻辑格式。

EEPROM 66 是在块基础上构成的,例如,在图 6 所示的实施例中,一个块是由 16 个字节组成的。

另外,在图 6 所示的实施例中,最上一个块的逻辑地址被设置为 #0000h(h 表示十六进制数),其它的逻辑地址按照增加的数字顺序分配。在图 6 中, #0000h 到 #FFFFh 被作为逻辑地址分配,如此构成 $65536 (= 2^{16})$ 个块。

多个块被构成,以使用做用户块或系统块。所述 EEPROM 66 的多个块被按照所述逻辑地址的增加数字顺序分配给所述用户块,按照逻辑地址的减少数字顺序分配给所述系统块。即,在图 6 中,所述用户块向下是增加的,而系统块向上是增加的。当没有空白块时,不能形成所述用户块和系统块。因此,在所述用户块和系统块之间的边界是不固定的,因此,对所述用户块的数量和所述系统块的数量没有强加限制(但是,在图 6 的实施例中,所述用

户块和系统块的总数被限制在 65536 或更少)。

所述系统块被划分成 5 种, 即, 制造 ID(识别)块、发行 ID 块、系统定义块、区域定义块和服务定义块。在图 6 所示的实施例中, 示出了作为区域/服务定义块的用做所述区域定义块或服务定义块的块。

- 5 在所述系统块以外, 在发行 IC 卡 2 时, 基本上已经设置了三种块, 即, 制造 ID 块、发行 ID 块和系统定义块, 它们被分别安排在逻辑地址 # FFFFh、# FF FEh 和 FF FDh 处。所述区域/服务定义块被以形成顺序设置在高于逻辑地址 # FF FCh 的逻辑地址处。

- 10 关于 IC 卡 2 的制造信息被设置在所述制造 ID 块内。即, 例如, 唯一的制造 ID、制造日期和制造代码等被设置在所述制造 ID 块内。

关于 IC 卡 2 的发行信息被设置在所述发行 ID 块内。即, 在所述发行 ID 块内设置有 IC 卡 2 的发行日期码以及 IC 卡 2 的发行顺序码等。

- 15 在所述系统定义块内, 设置有 EEPROM 66 拥有的系统块或用户块的数量以及系统密钥等。当在 IC 卡 2、R/W1 和控制器 3 之中执行相互确认时使用所述系统密钥。

区域定义块是通过向所述管理者分配 EEPROM 66 的存储区域(区域)形成的, 用于管理分配给所述管理者本身的存储区域的信息等被设置在所述区域定义块内。即, 例如在所述区域定义块内设置有下面将要描述的代码范围、空白容量、区域密钥等。

- 20 在所述服务定义块内, 设置有用于管理后面将要描述的服务区域(服务区域的容量、服务密钥等)的信息。

接着, 在定序器 91 中利用分层对 EEPROM 的存储区域进行管理。

即, 图 7 示出了 EEPROM 66 的目录结构。

- 25 在所述区域定义区域被分层的分层结构中指定了 EEPROM 66 的存储区域, 和指定所述区域定义区域, 以便能够具有一个区域定义区域和一个服务定义区域。

- 30 所述区域定义区域被分配给所述管理者。在所述区域定义区域中设置有表示识别码范围的代码范围, 所述识别码可被用做所述管理者用于识别所述区域定义区域和所述服务定义区域的名称, 还设置有用于表示可用的空白块数量的空白容量、用于产生后面将要描述的用于进行确认的一个访问密钥的一个区域密钥等。这里, 1 区域定义区域对应于结合图 6 所描述的 1 区域定

义块。

在图 7 的实施例中,分配给管理者 A 的所述区域定义区域构成了最上面的层,利用被设置为母层的所述管理者 A 的定义区域形成管理者 B1 和 B2 的区域定义区域。另外,利用被设置为母层的管理者 B1 的定义区域形成管理者 C 的区域定义区域。

所述服务定义区域被分配给由所述管理者提供的服务,用于存储提供服务所需数据的服务区域的容量、用于产生访问密钥的服务密钥等被设置在所述服务定义区域内。这里,1 服务定义区域对应于结合图 6 所描述的 1 服务定义块。

所述服务区域是一个用于存储提供服务所需数据的存储区域,它对应于图 6 所示的用户块。即,所述服务区域是由大于 0 个的用户块构成的,构成所述服务区域的用户块的数量被设置为用于管理所述服务区域的服务定义区域的容量。

另外,在所述区域定义区域和服务定义区域内设置有用于识别这些区域的识别码。这里,用于识别所述区域定义区域和所述服务定义区域的识别码此后被称之为区域码和服务码。所述服务码被用于识别用于管理一个服务区域的所述服务定义区域,由此,它可以被认为是一个用于识别所涉及服务区域的识别码(服务区域识别码)。

在图 7 所示的实施例中,最上层的所述区域定义区域被分配给管理者 A。0000h 到 FFFFh 被定义为可使用识别码的范围(代码范围),0123456789abcdef 被定义为区域密钥。这里,如果它是位于所述区域定义区域中的代码范围内的一个识别码,那么,任何一个识别码都可以被用做所述区域定义区域的区域码。在这个实施例中,所述区域定义区域的代码范围的最小值被用做它的区域码。因此,其代码范围从 0000h 到 FFFFh 的所述区域定义区域、即被分配给管理者 A 的区域定义区域的区域码被设置成 0000h。这里,其区域码被设置成 #xxxxh 的所述区域定义区域此后将被描述为区域定义区域 #xxxxh。

所述管理者 A 的区域定义区域 #0000h 的层被提供有一个其中所述管理者 A 提供服务的服务定义区域。区域定义区域 #0000h 的从 0000h 到 FFFFh 的所述代码范围的 0008h 被作为一个服务码分配给所述服务定义区域。这里,所述服务码 #xxxxh 的服务定义区域此后被描述为服务定义区域 #

xxxxh。

所述服务定义区域# 0008h 的容量被设置为 8，由此，可以使用由 8 个用户块构成的服务区域。另外，所述服务定义区域# 0008h 的服务密钥被设置为 0101010101010101。

5 所述管理者 A 的所述区域定义区域# 0000h 的层被提供有管理者 B1 的区域定义区域# 0100h 和管理者 B2 的区域定义区域# 1000h 作为子层。另外，所述区域定义区域# 0000h 的层被提供有其它的区域定义区域(未示出)，由此，例如，可被所述区域定义区域# 0000h 使用的块数量(空白容量)被设置为 37 个块。

10 在管理者 B1 的所述区域定义区域# 0100h 的代码范围被分配为从是所述区域定义区域# 0100h 的母层的所述区域定义区域# 0000h 的 0000h 到 FFFFh 的代码范围中的 0100h 到 03FFh 的情况下，由于管理者 B1 的所述区域定义区域的代码范围是从 0100h 到 03FFh，所以，是所述代码范围最小值的 0100h 被设置为管理者 B1 的所述区域定义区域的区域码。另外，所述区域定
15 义区域# 0100h 的空白容量和区域密钥被分别设置为 14 和 a0a0a0a0a0a0a0。

管理者 B1 的区域定义区域# 0100h 的层被提供有一个作为它的子层的管理者 C 的区域定义区域# 0300h。在管理者 C 的区域定义区域# 0300h 的代码范围被分配为是其母层的区域定义区域# 0100h 的从 0100h 到 03FFh 的代码范围中的 0300h 到 03FFh 的情况下，由于管理者 C 的所述区域定义区域的代码范围是从 0300h 到 03FFh，所以，是所述代码范围最小值的 0300h 被
20 设置为管理者 C 的所述区域定义区域的区域码。

所述区域定义区域# 0300h 的空白容量和区域密钥分别被设置为 0 和 b0b0b0b0b0b0b0b0。

25 管理者 C 的区域定义区域# 0300h 的层被提供有一个用于由管理者 C 提供服务的服务定义区域。在从区域定义区域# 0300h 的 0300h 到 03FFh 的代码范围中的 030Ch 被作为服务代码分配给所述服务定义区域。

被分配了所述服务代码 030Ch 的服务定义区域、即服务定义区域# 030Ch 的容量被设置为 16，然后，可以使用由 16 个用户块构成的服务区域。

30 另外，服务定义区域# 030Ch 的服务密钥被设置为 0202020202020202。

这里，由所述服务定义区域# 030Ch 管理的所述服务区域的容量等于

- 16, 和所述服务定义区域# 030Ch 本身使用一个块作为服务定义块, 这样, 由于所述服务定义区域# 030Ch 的存在, 正在被使用的块的数量等于 $17(= 16 + 1)$ 。由于其空白容量等于零, 所以, 可由所述服务定义区域# 030Ch 属于的一个层的所述区域定义区域# 0300h 使用的块的数量等于零。另外,
- 5 所述区域定义区域# 0300h 本身使用一个块作为一个区域定义块。因此, 在所述区域定义区域# 0300h 的层内, 正在被使用的块的数量等于 $18(= 17 + 1)$ 和可使用块的数量等于零。因此, 可以发现, 从用做它的母层(较上层)的区域定义区域# 0100h 分配的块的数量等于 $18(= 18 + 0)$ 。

- 关于区域定义区域# 0100h 的层, 如上所述, 在用做区域定义区域#
- 10 0100h 的子层(较下层)的区域定义区域# 0300h 中使用了 18 个块。另外, 所述区域定义区域# 0100h 本身使用一个块作为区域定义块。所述区域定义区域# 0100h 的空白容量等于 14。因此, 在区域定义区域# 0100h 的层中, 正在被使用的块的数量等于 $19(= 18 + 1)$, 和可被使用的块的数量等于 14。因此, 从用做其母层的区域定义区域# 0000h 分配的块的数量等于 $33(= 19$
- 15 $+ 14)$ 。

- 相反, 在管理者 B2 的区域定义区域# 1000h 的代码范围被分配为在用做其母层的区域定义区域# 0000h 的从 0000h 到 FFFFh 的代码范围中的 1000h 到 1FFFh 的情况下, 由于管理者 B2 的区域定义区域的代码范围是从 1000h 到 1FFFh, 因此, 是上述代码范围最小值的 1000h 被设置为管理者 B2 的所
- 20 述区域定义区域的区域码。

另外, 区域定义区域# 1000h 的空白容量和区域密钥分别被设置为 43 和 c0c0c0c0c0c0c0c0。

- 管理者 B2 的区域定义区域# 1000h 的层被提供有用于提供管理者 B2 服务的一个服务定义区域。在区域定义区域# 1000h 的从 1000h 到 1FFFh 的代码范围中的 1022h 被作为一个服务码分配给所述服务定义区域。
- 25

被分配了服务码 1022h 的服务定义区域、即服务定义区域# 1022h 的容量被设置为 4, 和由此可以使用由 4 个用户块构成的一个服务区域。另外, 服务定义区域# 1022h 的服务密钥被设置为 0303030303030303。

- 这里, 由所述服务定义区域# 1022h 管理的所述服务区域的容量等于
- 30 4, 和服务定义区域# 1022h 本身使用一个块作为服务定义块, 因此, 由于存在所述服务定义区域# 1022h, 所以, 正在被使用的块的数量等于 $5(= 4$

+ 1)。另外，由于其空白容量等于 43，所以，可被服务定义区域# 1022h 属于的层的区域定义区域# 1000h 使用的块的数量等于 43。另外，区域定义区域# 1000h 本身使用一个块作为区域定义块。因此，在所述区域定义区域# 1000h 的层中，正在被使用的块的数量等于 $6(= 5 + 1)$ ，和可被使用块的数量等于 43，因此，被分配给区域定义区域# 1000h 的块的数量等于 $49(= 6 + 43)$ 。

由于如上所述被用做能够被分配给将被管理的一个区域定义区域的识别码的范围的代码范围被存储在所述区域定义区域中，所以，可以在所述代码范围的基础上定义图 7 所示的这种层结构，在这种层结构中，一个管理目标的区域定义区域被设置为子层，而用于管理该区域定义区域的区域定义区域被设置为母层。

下面，结合附图 8 描述在假设被分配给了最上层的区域定义区域# 0000h 的管理者 A 是一个 IC 卡 2 的提供者的前提下构成图 7 所示层结构的处理。

管理者 A 根据用户的请求发行所述 IC 卡 2 (1)。在所述 IC 卡 2 中只形成图 7 所示层结构的区域定义区域# 0000h。

当管理者 A 通过使用由所述服务定义区域# 0008h 管理的所述服务区域开始提供预定的服务时，管理者 A 将形成所述服务定义区域# 0008h 所需的信息登录到已登录卡的发卡机 101 中(2)。

这里，已登录卡的发卡机 101 例如是由图 3 所述的 R/W1 和控制器 3 构成的。已登录卡的发卡机 101 可以被设置在火车站、零售店或其它方便的地方。

此后，当用户将 IC 卡 2 插入到已登录卡的发卡机 101 中时(当 IC 卡 2 被设置得将被允许与包含在已登录卡的发卡机 101 中的 R/W1 通信时)，已登录卡的发卡机 101 执行已登录卡的发行工作，即，在已登录的信息的基础上传送一个命令和必要的信息给 IC 卡 2 以形成所述服务定义区域# 0008h。经过上述操作，所述用户被允许通过使用由服务定义区域# 0008h 管理的所述服务区域接受由管理者 A 提供的服务。

相反，当管理者 B1、B2 试图使用 IC 卡 2 被提供服务时，他们中的每一个与管理者 A 订立合同，从而使管理者 A 将形成区域定义区域# 0100h 和# 1000h 所需的信息登录到已登录卡的发卡机 101 中(3)，(4)。当用户将 IC 卡 2 插入到已登录卡的发卡机 101 中时，已登录卡的发卡机 101 执行已登录

卡的发行工作,即,在已登录的信息的基础上向 IC 卡 2 传送一个命令和必要的数据以形成区域定义区域# 0100h 和# 1000h,借此,管理者 B1 或 B2 能够使用在区域定义区域# 0100h 或# 1000h 中定义的所述范围内的 IC 卡 2 的资源。在这种情况下,管理者 B1 和 B2 的已登录卡的发行经营者是管理者 A。

此后,当管理者 B2 通过使用由服务定义区域# 1022h 管理的服务区域开始提供预定服务时,管理者 B2 将形成服务定义区域# 1022h 所需的信息登录到已登录卡的发卡机 101 中(5)。当用户将 IC 卡 2 插入到已登录卡的发卡机 101 中时,已登录卡的发卡机 101 在已登录信息的基础上向 IC 卡 2 传送一个命令和必要的数据以形成服务定义区域# 1022h。因此,所述用户可以使用由服务定义区域# 1022h 管理的所述服务区域被提供管理者 B2 的服务。

另外,当管理者 C 希望在管理者 B1 的管理下经过 IC 卡 2 提供服务时,管理者 C 与管理者 B1 订立一个合同,从而使管理者 B1 将形成区域定义区域# 0300h 所需的信息登录到已登录卡的发卡机 101 中(6)。当用户将 IC 卡 2 插入到已登录卡的发卡机 101 中时,已登录卡的发卡机 101 在已登录信息的基础上向 IC 卡 2 传送一个命令和必要的数据以形成区域定义区域# 0300h,借此,管理者 C 能够使用在区域定义区域# 0300h 中定义的所述范围内的 IC 卡 2 的资源。在这种情况下,管理者 C 的已登录卡的发行经营者是管理者 B1。

此后,当管理者 C 通过使用由服务定义区域# 030Ch 管理的服务区域开始提供预定服务时,管理者 C 将形成服务定义区域# 030Ch 所需的信息登录到已登录卡的发卡机 101 中(7)。当用户将 IC 卡 2 插入到已登录卡的发卡机 101 中时,已登录卡的发卡机 101 在已登录信息的基础上传送一个命令和必要的数据到 IC 卡 2 以形成服务定义区域# 030Ch,借此,所述用户能够使用由服务定义区域# 030Ch 管理的服务区域接受由管理者 C 提供的服务。

如上所述,在 IC 卡 2 中,根据来自已登录卡的发卡机 101 的命令形成所述区域定义区域和服务定义区域。形成区域定义区域的区域形成处理和形成服务定义区域的服务形成处理例如是由定序器 91 执行的。下面将结合图 9 和 10 描述所述区域形成处理和所述服务形成处理。

首先,结合图 9 的流程描述所述区域形成处理。

当 IC 卡 2 被插入到已登录卡的发卡机 101 中时, 已登录卡的发卡机 101 向 IC 卡 2 传送例如一个用于指令形成一个区域定义区域的命令(此后, 作为定义, 该命令被称之为形成命令)、形成所述区域定义区域所必要的信息, 即、要被形成的所述区域定义区域的代码范围、被分配给所述区域定义区域的块的数量(此后称之为分配块数)和区域密钥。

当接收所述区域形成命令时, IC 卡 2(定序器 91)识别与所述区域形成命令一起传送的要被形成的区域定义区域的代码范围、分配块数和区域密钥等。另外, 在 IC 卡 2 中, 识别要被形成的所述区域定义区域的区域码。即, 在这种情况下, 要被形成的所述区域定义区域的代码范围的最小值被识别为它的区域码。另外, 在 IC 卡 2 中, 具有包含要被形成的所述区域定义区域的代码范围的所述代码范围的区域定义区域被识别为要被形成的区域定义区域的母层的区域定义区域。

在 IC 卡 2 中, 在步骤 S1 判断在 EEPROM 66 中是否已经形成了要被形成的区域定义区域。即, 在步骤 S1 中, 判断具有与要被形成的所述区域定义区域的区域码相同区域码的区域定义区域是否已经被形成。

如果在步骤 S1 的判断结果是要被形成的所述区域定义区域已经被形成, 那么, 所述区域形成处理结束。即, 在所述要被形成的区域定义区域已经被形成的情况下, 由于不需要重复形成相同的区域定义区域, 所以, 不再执行以后的处理。

如果在步骤 S1 的判断结果是要被形成的区域定义区域还没有被形成, 处理前进到步骤 S2 以判断要被形成的所述区域定义区域的代码范围和被分配块的数量(容量)是否合适。即, 在步骤 S2 判断要被形成的区域定义区域的代码范围是否被包含在存储在母层的区域定义区域内的代码范围内和要被形成的区域定义区域的分配块数是否低于存储在母层的区域定义区域内的空白容量。

当在步骤 S2 判断要被形成的区域定义区域的代码范围和分配块数不合适时, 即, 当要被形成的区域定义区域的代码范围被包含在存储在所述母层的区域定义区域内的代码范围中或要被形成的区域定义区域的分配块数超过了存储在所述母层的区域定义区域内的空白容量时, 在步骤 S3 执行一个差错处理和然后区域形成处理结束。即, 在步骤 S3, 其中没有区域定义区域可以被作为所述母层的区域定义区域的子层而形成的一个消息被传送给已登

录卡的发卡机 101。因此,在这种情况下,没有区域定义区域形成(不执行已登录卡的发行工作)。

相反,如果在步骤 S2 的判断结果是要被形成的所述区域定义区域的代码范围和分配块数是合适的,即,它判断要被形成的区域定义区域的代码范围被包含在存储在所述母层的所述区域定义区域内的代码范围中和要被形成的区域定义区域的分配块数低于存储在所述母层的区域定义区域中的空白容量,那么,在步骤 S4,所述要被形成的区域定义区域被形成作为所述母层的区域定义区域的子层。

即,在步骤 S4,在 EEPROM 66(图 6)的空白块中的最低块(具有最大逻辑地址的空白块)被保证作为与要被形成的区域定义区域对应的区域定义块。另外,所述代码范围、空容量和区域密钥等被写入(存储)到所述区域定义块中。这里,在步骤 S4 中,从已登录卡的发卡机 101 传送的数据被作为所述区域码和区域密钥直接写入。从由已登录卡的发卡机 101 传送的所述分配块数中减去 1 所获得的值被作为所述空白容量写入。由于如此形成的所述区域定义区域使用一个块,所以,从所述分配块数中减去 1 所获得的值被写入。

然后,所述处理进入到步骤 S5 以改写所述母层的区域定义区域的空白容量,然后,所述区域形成处理结束。即,在步骤 S5 中,从所述母层的区域定义区域的空白容量中减去所述分配块数所获得的值被作为所述母层的区域定义区域的空白容量重新写入。

图 7 所示的管理者 B1、B2、C 的区域定义区域 # 0100h、# 1000h 和 # 0300h 是通过上述区域形成处理形成的。

即,假设在发行 IC 卡 2 时,也是 IC 卡 2 发行者的管理者 A 具有 IC 卡 2 的所有资源和识别代码或可由 IC 卡 2 使用的容量是从 0000h 到 FFFFAh 或 65533 个块,那么,在发行 IC 卡 2 时,只有其中代码范围是从 0000h 到 FFFFh 且其空白容量等于 65532 的最上层的区域定义区域 # 0000h 作为一个区域定义区域存在。

在这个实施例中,如图 6 所示,EEPROM 66 具有 65536 个块,但是,由于制造 ID 块、发行 ID 块和系统定义块的存在,在刚刚发行 IC 卡 2 之后其可使用的容量等于其数量比 65536 少 3 的 65533 个块。

另外,所述最上层的区域定义区域 # 0000h 的空白容量等于 65532 个

块, 由于所述区域定义区域 # 0000h 本身使用一个块, 所以, 该数量比可使用容量 65533 个块少一个块。

当管理者 A 向管理者 B1 分配位于从 0100h 到 03FFh 范围中的识别码和其资源中的 33 个块时, 执行所述区域形成处理以形成区域定义区域 # 0100h。即, 在这种情况下, 0100h 到 03FFh 和 32 个块被分别作为一个代码范围和一个空白容量写入到区域定义区域 # 0100h 中。由于区域定义区域 # 0100h 本身使用一个块, 所以, 所述空白容量的数量比从管理者 A 分配的 33 个块少一个块。

当形成区域定义区域 # 0100h 时, 管理者 A 的区域定义区域 # 0000h 的空白容量被减少分配到管理者 B1 的 33 个块。

当管理者 A 向管理者 B2 分配位于从 1000h 到 1FFFh 的范围内的识别码和 49 个块时, 执行所述区域形成处理, 以形成区域定义区域 # 1000h。即, 在这种情况下, 1000h 到 1FFFh 和 48 个块被分别作为一个代码范围和一个空白容量写入到区域定义区域 # 1000h 中。由于区域定义区域 # 1000h 本身使用一个块, 所以, 所述空白容量比从管理者 A 分配的 49 个块少一个块。

当形成区域定义区域 # 1000h 时, 管理者 A 的区域定义区域 # 0000h 的空白容量被减少分配到管理者 B2 的 49 个块。

当如上所述形成区域定义区域 # 0100h 或 # 1000h 时, 管理者 B1 或 B2 被允许在区域定义区域 # 0100h 或 # 1000h 的层中形成作为上层的子层的一个区域定义区域和一个服务定义区域。

例如, 当管理者 B1 向管理者 C 分配从 0300h 到 03FFh 范围的识别码和 18 个块时, 执行所述区域形成处理以形成区域定义区域 # 0300h。即, 在这种情况下, 0300h 到 03FFh 和 17 个块被作为一个代码范围和一个空白容量写入到区域定义区域 # 0300h 中。由于区域定义区域 0300h 本身使用一个块, 所以, 所述空白容量比从管理者 B1 分配的 18 个块少一个块。

当形成区域定义区域 # 0300h 时, 管理者 B1 的区域定义区域 # 0100h 的空白容量被减少分配到管理者 C 的 18 个块。即, 如上所述, 当形成区域定义区域 # 0100h 时, 区域定义区域 # 0100h 的空白容量等于 32 个块。但是, 如图 7 所示, 从所述空白容量中减掉 18 个块, 所以所述空白容量等于 14 个块。

下面将结合图 10 的流程描述服务形成处理。

当 IC 卡 2 被插入到已登录卡的发卡机 101 中时, 已登录卡的发卡机 101 向 IC 卡 2 传送一个指令形成服务定义区域的命令(此后称之为服务形成命令)以及形成所述服务定义区域所需的信息, 即, 要被形成的服务定义区域的服务码、分配给所述服务定义区域的块数(此后称之为分配块数)和服务密钥等。

当接收到所述服务形成命令时, IC 卡 2(定序器 91)识别要被形成的服务定义区域的服务码、分配块数和服务密钥等。另外, 在 IC 卡 2 中, 具有包含要被形成的所述服务定义区域的服务码的代码范围的区域定义区域被识别为要被形成的所述服务定义区域的母层的区域定义区域。

10 在 IC 卡 2 中, 在步骤 S11 判断在 EEPROM 66 中是否已经形成了所述要被形成的服务定义区域。即, 在步骤 S11 判断与所述要被形成的服务定义区域具有相同服务码的服务定义区域是否已经形成。

当在步骤 S11 的判断结果是已经形成了要被形成的所述服务定义区域时, 所述服务形成处理结束。即, 当要被形成的服务定义区域已经被形成时, 15 由于不需要重复形成相同的服务定义区域, 所以不再执行随后的处理。

另外, 如果在步骤 S11 判断的结果是还没有形成要被形成的服务定义区域, 则所述处理进入到步骤 S12 以判断要被形成的服务定义区域的服务码和所述分配块数(容量)是否是合适的。即, 在步骤 S12 判断要被形成的服务定义区域的服务码是否被包含在存储在所述母层的区域定义区域中的代码范围 20 内和所述要被形成的服务定义区域的分配块数是否低于存储在所述母层的区域定义区域中的空白容量。

如果在步骤 S12 的判断结果是要被形成的服务定义区域的服务码和所述分配块数是不合适的, 即, 如果要被形成的服务定义区域的服务码没有被包含在存储在所述母层的区域定义区域中的代码范围内或要被形成的服务定义区域的分配块数超过了存储在所述母层的区域定义区域中的空白容量, 处理 25 进入到步骤 S13 以执行差错处理, 然后所述区域形成处理结束。即, 在步骤 13 中, 在所述母层的区域定义区域的层中不能形成服务定义区域的一个消息被传送给已登录卡的发卡机 101。因此, 在这种情况下, 不能形成服务定义区域。

30 相反, 如果在步骤 S12 的判断结果是要被形成的服务定义区域的服务码和所述分配块数是合适的, 即, 如果要被形成的服务定义区域的服务码被包

含在存储在所述母层的区域定义区域中的代码内和所述要被形成的服务定义区域的分配块数低于存储在所述母层的区域定义区域中的空白容量，处理进入到步骤 S14，在这个步骤 S14 中，在所述母层的区域定义区域的层中形成所述服务定义区域。

- 5 即，在步骤 S14 中，在 EEPROM 66(图 6)的空白块中的最低块(具有最大逻辑地址的空白块)被保证作为与要被形成的服务定义区域对应的服务定义块。另外，所述服务码、容量和服务密钥等被写入到所述服务定义块中。在这种情况下，在步骤 S14 中，从已登录卡的发卡机 101 传送的服务码和服务密钥等被直接写入。从由已登录卡的发卡机 101 传送的分配块数中减掉 1 所
10 获得的值被作为所述容量写入。由于要被形成的服务定义区域使用一个块，所以，从所述分配块数中减掉 1 所获得的值被写入。

在步骤 S14 中，以逻辑地址增加的顺序选择其数量对应于在被如此形成的服务定义区域中写入的容量的空白块，并保证作为构成由所述服务定义区域管理的服务区域的用户块。此后，所述处理前进到步骤 S15。

- 15 在步骤 S15 中，改写所述母层的区域定义区域的空白容量，和所述服务形成处理结束。即，在步骤 S15 中，从所述母层的区域定义区域的空白容量中减掉所述分配块数所获得的值被作为所述区域定义区域的空白容量重新写入。

- 20 通过执行上述服务形成处理，形成图 7 所示管理者 A、B2、C 的服务定义区域 # 0008h、# 1022h 和 # 030Ch。

- 即，当管理者 A 使用 0008h 的识别码和在它的资源中的 9 个块的容量提供它的服务时，执行所述服务形成处理，以形成服务定义区域 # 0008h，并将 8 个块作为一个容量写入到所述服务定义区域 # 0008h 中。另外，8 个空白块被保证用做用户块和设置为由所述区域定义区域 # 0008h 管理的服
25 务区域。由于服务定义区域 # 0008h 使用一个块，所以，写入到服务定义区域 # 0008h 中的容量少于 9 个块的数量。

当形成服务定义区域 # 0008h 时，管理者 A 的区域定义区域 # 0000h 的空白容量被减少了分配给服务定义区域 # 00008h 的 9 个块。

- 如上所述，管理者 A 能够使用由所述服务定义区域 # 0008h 管理的 8 个
30 块的服务区域提供服务。

当管理者 B2 使用 1022h 的识别码和在其资源中的 5 个块的容量提供服

务时，执行所述服务形成处理以形成服务定义区域# 1022h，和4个块作为一个容量被写入到所述服务定义区域# 1022h中。另外，4个空白块被保证作为用户块和它被设置为由所述服务定义区域# 1022h管理的服务区域。由于所述服务定义区域# 1022h本身使用一个块，所以，写入到服务定义区域# 5 1022h中的容量比所述的5个块少一个块。

当形成所述服务定义区域# 1022h时，管理者B2的区域定义区域# 1000h的空白容量被减掉分配给服务定义区域# 1022h的5个块。即，如上所述，在形成区域定义区域# 1000h时，所述空白容量等于48个块，但是，它被减少了5个块和如图7所示等于43个块。

10 如上所述，管理者B2被允许使用由所述服务定义区域# 1022h管理的4个块的服务区域提供服务。

另外，当管理者C使用例如030Ch的识别码和在它的资源中的17个块的容量提供服务时，执行所述服务形成处理以形成服务定义区域# 030Ch，和16个块被作为一个容量写入到服务定义区域# 030Ch中。另外，16个空
15 白块被保证作为用户块，和它被设置为由所述区域定义区域# 030Ch管理的一个服务区域。由于服务定义区域# 030Ch本身使用一个块，所以，在所述服务定义区域# 030Ch中写入的容量比17个块的数量少一个块。

当形成服务定义区域# 030Ch时，管理者C的区域定义区域# 0300h的空白容量被减少分配给所述服务定义区域# 030Ch的17个块。即，如上
20 所述，当形成区域定义区域# 0300h时，所述空白容量等于17个块，但是，它被减少了17个块和如图7所示等于零。

如上所述，管理者C被允许使用由所述服务定义区域# 030Ch管理的16个块的服务区域提供服务。

如上所述，EEPROM 66是在其中存储了所述代码范围和所述空白容量的
25 的所述区域定义区域的基础上被管理的，因此，可以执行IC卡2的资源管理。即，可在一个区域定义区域的层中可使用的容量和识别码能够受到限制。作为结果，即使当一个管理者将分配给它的部分资源(在这种情况下是可用的容量和识别码)分配给另一个管理者从而使IC卡2可被共同使用时，也可以避免所述识别码在不同的使用者之间重叠和所述管理者可以避免使用超过通过
30 合同等预定的容量的EEPROM 66。

在IC卡2中，EEPROM 66的存储区域具有一个层结构，在这个结构

中, 所述区域定义区域如结合图 7 所述分层, 并且用于确认的密钥(在这个实施例中, 用于区域定义区域的密钥和用于服务定义区域的密钥分别被称之为区域密钥和服务密钥)被分别存储在所述区域定义区域和所述服务定义区域中, 因此, 可以对所述 IC 卡 2 执行高度灵活和安全的访问控制。

- 5 即, 通过在多个管理者之间传送图 11 所示的信息, 可以对 IC 卡 2 执行高度灵活和安全的访问控制。

特别是, 作为 IC 卡 2 发行者的管理者 A 确定要被存储在 EEPROM 66 的系统定义块(图 6)中的系统密钥和区域定义区域 # 0000h 本身的区域密钥, 并在将所述区域密钥 # 0000h 存储到区域定义区域 # 0000h 中的同时将所述
10 系统密钥存储到所述系统定义块中。这里, 区域定义区域 # xxxxh 的区域密钥此后被称之为区域密钥 # xxxxh。

另外, 管理者 A 利用区域密钥 # 0000h 加密所述系统密钥并产生一个区域中间密钥 K_A 。DES(数据加密标准)、FEAL(快速数据加密算法)等可以被用做加密方法。

- 15 当管理者 A 将它的资源分配给管理者 B1 时, 管理者 A 将所述区域中间密钥 K_A 给予管理者 B1。另外, 管理者 A 确定管理者 B1 的区域密钥 # 0100h 并将这个密钥与它的区域码 # 0000h 一起给予(分配给)管理者 B1。

因此, 管理者 B1 能够识别所述区域中间密钥 K_A 和它的区域密钥 # 0100h, 但是, 它不能识别是所谓母层的管理者 A 的系统密钥和区域密钥 #
20 0000h。但是, 管理者 B1 的区域密钥 # 0100h 被给予用做作为母层的管理者 A 的子层的管理者 B1, 然后, 用做母层的管理者 A 识别作为子层的管理者 B1 的区域密钥 # 0100h。

由管理者 A 给予管理者 B1 的所述区域密钥 # 0100h 经过管理者 B1 的区域定义区域 # 0100h 的区域形成处理(图 9)被写入到所述区域定义区域 #
25 0100h。

管理者 B1 在从管理者 A 获得的区域密钥 # 0100h 的基础上加密从用做其母层的管理者 A 获得的所述区域中间密钥 K_A 以产生一个区域中间密钥 K_{B1} 。

- 30 当管理者 A 将它的资源分配给管理者 B2 时, 它还将所述区域中间密钥 K_A 给予管理者 B2。另外, 管理者 A 确定管理者 B2 的区域密钥 # 1000h, 并将该区域密钥 # 1000h 与它的区域码 # 0000h 一起给予管理者 B2。

因此，管理者 B2 能够识别所述区域中间密钥 K_A 和它的区域密钥 # 1000h，但是，不能识别所述系统密钥和用做母层的管理者 A 的区域密钥 # 0000h。但是，由于管理者 B2 的区域密钥 # 1000h 被用做母层的管理者 A 给予了作为子层的管理者 B2，所以，用做母层的管理者 A 能够识别作为子层的管理者 B2 的区域密钥 # 1000h。

在管理者 B2 的区域定义区域 # 1000h 的区域形成处理中，由管理者 A 给予管理者 B2 的区域密钥 # 1000h 被写入到它的区域定义区域 # 1000h 中。

管理者 B2 在从管理者 A 获得的区域密钥 # 1000h 的基础上加密从作为母层的管理者 A 获得的区域中间密钥 K_A 以产生一个区域中间密钥 K_{B2} 。

相反，当管理者 B1 将它的资源分配给管理者 C 时，管理者 B1 将所述区域中间密钥 K_{B1} 给予管理者 C。另外，管理者 B1 确定管理者 C 的区域密钥 # 0300h 并将这个密钥连同它的区域码 # 0100h 和用做母层的管理者 A 的区域码 # 0000h 一起给予管理者 C。

因此，管理者 C 能够识别所述区域中间密钥 K_{B1} 和它的区域密钥 # 0300h，但是，不能识别用做母层的管理者 B1 的区域密钥 # 0100h。但是，由于区域密钥 # 0100h 已经由作为母层的管理者 B1 给予了作为子层的管理者 C，所以，用做母层的管理者 B1 能够识别作为子层的管理者 C 的区域密钥 # 0300h。

由管理者 B1 给予管理者 C 的区域密钥 # 0300h 经过管理者 C 的区域定义区域 # 0300h 的区域形成处理被写入到它的区域定义区域 # 0300h 中。

管理者 C 在从管理者 B1 获得的区域密钥 # 0300h 的基础上加密从用做母层的管理者 B1 获得的区域中间密钥 K_{B1} 以产生区域中间密钥 K_C 。

当管理者 A 使用由在它的区域定义区域 # 0000h 的层中形成的服务定义区域 # 0008h 管理的所述服务区域提供它的服务时，如图 12 所示，管理者 A 在所述区域中间密钥 K_A 的基础上加密存储在服务定义区域 # 0008h 中的服务密钥(存储在服务定义区域 # xxxxh 中的服务密钥此后被称之为服务密钥 # xxxxh)以产生服务中间密钥 K_{*0008h} 和将其与区域中间密钥 K_A 一起登录到服务提供机 111 中。另外，管理者 A 将它的区域定义区域 # 0000h 的区域码 # 0000h 和在区域定义区域 # 0000h 的层中形成的服务定义区域 # 0008h 的服务码 # 0008h 登录到所述服务提供机 111 中。

这里，所述服务提供机 111 例如是由图 3 所示的 R/W1 和控制器 3 构成

的, 和数据被从/向一个预定的区域读出/写入以提供一个预定的服务。

在这种情况下, 当 IC 卡 2 被插入到所述服务提供机 111 中时, 在所述服务提供机 111 和 IC 卡 2 之间执行后续的相互确认。

即, 图 13 所示的服务提供机 111 向 IC 卡 2 传送所述登录的区域码 # 0000h 和服务码 # 0008h。在 IC 卡 2(定序器 91)中, 接收来自所述服务提供机 111 的区域码 # 0000h 和服务码 # 0008h。

在 IC 卡 2 中, 存储在所述系统定义块(图 6)中的系统密钥被读出, 并从具有从服务提供机 111 接收的区域码 # 0000h 的区域定义区域中读出区域密钥 # 0000h。另外, 在区域密钥 # 0000h 的基础上加密所述系统密钥, 从而产生与登录在图 12 所示服务提供机 111 中的所述区域中间密钥 K_A 相同的密钥。与所述区域中间密钥 K_A 相同的密钥被设置为用于确认的第一访问密钥(确认密钥) K_{bc} 。

在 IC 卡 2 中, 从具有从所述服务提供机 111 接收的服务码 # 0008h 的服务定义区域中读出所述服务密钥 # 0008h。在服务密钥 # 0008h 的基础上加密区域中间密钥 K_A , 从而产生与登录在图 12 所示服务提供机 111 中的服务中间密钥 $K_{\#0008h}$ 相同的密钥。与服务中间密钥 $K_{\#0008h}$ 相同的密钥被设置为用于确认的第二访问密钥 K_{ac} 。

因此, 在这种情况下, 用做第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的区域中间密钥 K_A 或服务中间密钥 $K_{\#0008h}$ 被登录到所述服务提供机 111 中, 借此, 在 IC 卡 2 中产生用做第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的区域中间密钥 K_A 或服务中间密钥 $K_{\#0008h}$ 。

例如, 如图 14 所示, 服务提供机 111 确认 IC 卡 2。

即, 在服务提供机 111 中, 产生一个随机数, 并根据算法 E1 对其进行转换。即, 在第二访问密钥 K_{ac} 的基础上加密(例如, DES 加密)所述随机数, 和在所述第一访问密钥 K_{bc} 的基础上译码(例如, DES 译码)所述加密结果。在所述第二访问密钥 K_{ac} 的基础上加密译码结果。在算法 E1 的基础上对所述随机数的转换结果被传送给 IC 卡 2。

在 IC 卡 2 中, 根据算法 D1 对来自服务装置 111 的以算法 E1 为基础对所述随机数进行转换的结果进行转换。即, 在第二访问密钥 K_{ac} 的基础上, 译码在算法 E1 基础上的转换结果, 和在所述第一访问密钥 K_{bc} 的基础上加密所述译码结果。另外, 在所述第二密钥 K_{ac} 的基础上译码所述加密结果。

在 IC 卡 2 中，根据算法 E2 对在算法 D1 基础上的转换结果做进一步的转换。即，在所述第一访问密钥 K_{bc} 的基础上加密在算法 D1 基础上的转换结果，和在第二加密密钥 K_{ac} 的基础上加密所述第一访问密钥 K_{bc} 。在第一访问密钥 K_{bc} 的第二访问密钥 K_{ac} 的基础上的加密结果基础上，译码用于在算法 D1 基础上的转换结果的在第一访问密钥 K_{bc} 基础上的加密结果。在所述第一访问密钥 K_{bc} 的基础上加密译码结果并传送给服务提供机 111。

在所述服务提供机 111 中，根据算法 D2 对来自 IC 卡 2 以算法 E2 为基础的转换结果进行转换。即，在所述第一访问密钥 K_{bc} 的基础上对在算法 E2 基础上的转换结果进行译码，和在第二访问密钥 K_{ac} 的基础上加密所述第一访问密钥 K_{bc} 。在所述第二访问密钥 K_{ac} 的基础上的所述第一访问密钥 K_{bc} 的加密结果的基础上，加密用于在算法 E2 基础上的转换结果的在所述第一访问密钥 K_{bc} 的基础上的译码结果。在所述第一访问密钥 K_{bc} 的基础上译码所述加密结果。

在服务提供机 111 中，原来的随机数和以算法 D2 为基础的转换结果彼此进行比较以确认 IC 卡 2。即，当原来的随机数与以算法 E2 为基础的转换结果相符合时，它被识别为所述 IC 卡 2 是合适的。相反，如果它们彼此不相符合，则所述 IC 卡 2 被认为是不合适的(例如，它被伪造的)。

例如，如果 IC 卡 2 被识别为是合适的，如图 15 所示在 IC 卡 2 中执行服务提供机 111 的确认。

即，在 IC 卡 2 中，产生一个随机数，并且根据算法 E2 对所述随机数进行转换和传送给服务提供机 111。

在服务提供机 111 中，根据算法 D2 对在来自 IC 卡 2 的算法 E2 的基础上的所述随机数的转换结果进行转换。并根据算法 E1 对在算法 D2 基础上的转换结果进行转换和传送给 IC 卡 2。

在 IC 卡 2 中，根据算法 D1 对在来自服务提供机 111 的在算法 E1 基础上的转换结果转换，和所述转换结果与原来的随机数彼此之间进行比较以执行与服务提供机 111 相关的确认。即，当原来的随机数与在算法 D2 基础上的转换结果相符时，所述服务提供机 111 被识别为是合适的。相反，如果它们彼此之间不相符合，所述服务提供机 111 被识别为是不合适的(例如，被修改)。

当 IC 卡 2 和所述服务提供机 111 都被识别为是合适的时，在 IC 卡 2 中

允许仅对由具有从所述服务提供机 111 传送的服务码的服务定义区域管理的
服务区域进行访问。因此，在结合图 12 和 13 描述的情况下，可以仅对由服
务定义区域 # 0008h 管理的服务区域进行访问。

即，知道所述区域中间密钥 K_A 、所述区域码 0000h、所述服务密钥 #
5 0008h 和所述服务码 # 0008h 的管理者 A 能够访问由服务定义区域 # 0008h
管理的服务区域。但是，管理者 A 既不知道服务密钥 # 1022h，也不知道服
务密钥 # 030Ch，所以，它基本上不能对由服务定义区域 # 1022h 或 # 030Ch
管理的服务区域进行访问。

接着，当管理者 B2 使用由在它的区域定义区域 # 1000h 的层中形成的
10 服务定义区域 # 1022h 管理的服务区域提供它的服务时，如图 16 所示在所述
区域中间密钥 K_{B2} 的基础上加密存储在服务定义区域 # 1022h 中的服务密钥
1022h，以产生服务中间密钥 $K_{\#1022h}$ 和将它与区域中间密钥 K_{B2} 一起登录
到服务提供机 111 中。管理者 B2 将在它的区域定义区域 # 1000h 的层的上
面的较上层的区域定义区域的区域码，即，在这种情况下，是管理者 A 的区
15 域定义区域 # 0000h 的区域码 # 0000h 和它的区域定义区域 # 1000h 的区域
码 # 1000h 以及在区域定义区域 # 1000h 的层中形成的服务定义区域 #
1022h 的服务码 # 1022 登录到服务提供机 111 中。

在这种情况下，当 IC 卡 2 被插入到服务提供机 111 中时，在服务提供
机 111 和 IC 卡 2 之间执行随后的相互确认。

20 即，如图 17 所示，服务提供机 111 向 IC 卡 2 传送已登录的区域码 # 0000h
和 # 1000h 和服务码 # 1022h。在 IC 卡 2(定序器 91)中，从服务提供机 111
中接收区域码 # 0000h 和 # 1000h 和服务码 # 1022h。

在 IC 卡 2 中，读出存储在系统定义块(图 6)中的系统密钥，和从具有从
服务提供机 111 中接收的区域码 # 0000h 或 # 1000h 的区域定义区域中读出
25 区域密钥 # 0000h 或 # 1000h。另外，在区域密钥 # 0000h 的基础上加密所述
系统密钥，从而产生与所述区域中间密钥 K_A 相同的密钥。在区域密钥 # 1000h
的基础上加密与所述区域中间密钥 K_A 相同的密钥，从而产生图 16 所示与被
登录在所述服务提供机 111 中的区域中间密钥 K_{B2} 相同的密钥。与所述区域
中间密钥 K_{B2} 相同的密钥被设置为用于确认的第一访问密钥 K_{bc} 。

30 在 IC 卡 2 中，从具有从服务提供机 111 中接收的服务码 # 1022h 的服务
定义区域中读出服务密钥 # 1022h。在所述服务密钥 # 1022h 的基础上加密

与所述区域中间密钥 K_{B2} 相同的密钥,从而产生与登录在图 16 所示服务提供机 111 中的服务中间密钥 $K_{\#1022h}$ 相同的密钥。与服务中间密钥 $K_{\#1022h}$ 相同的密钥被设置为用于确认的第二访问密钥 K_{ac} 。

因此,在这种情况下,是所述第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的所述区域中间密钥 K_{B2} 或所述服务中间密钥 $K_{\#1022h}$ 被登录在服务提供机 111 中,和在 IC 卡 2 中,产生是所述第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的所述区域中间密钥 K_{B2} 或所述服务中间密钥 $K_{\#1022h}$ 。

和在结合图 14 和 15 所述的情况相同,在 IC 卡 2 和服务提供机 111 之间执行相互确认。

作为所述相互确认的结果,当 IC 卡 2 和服务提供机 111 都被识别为是合适的时,允许在 IC 卡 2 中仅对由具有从服务提供机 111 传送的服务码的服务定义区域管理的服务区域进行访问。因此,在图 16 和 17 的情况下,可以仅对由服务定义区域 $\#1022h$ 管理的服务区域进行访问。

即,知道所述区域中间密钥 K_{B2} 、所述区域码 $\#0000h$ 、 $\#1000h$ 、所述服务密钥 $\#1022h$ 和所述服务码 $\#1022h$ 的管理者 B2 能够访问由服务定义区域 $\#1022h$ 管理的服务区域。但是,管理者 B2 既不知道服务密钥 $0008h$ 也不知道 $\#030Ch$, 所以,它基本不能访问由服务定义区域 $\#0008h$ 和 $\#030Ch$ 管理的服务区域。

接着,当管理者 C 使用由在它的区域定义区域 $\#0300h$ 的层中形成的服务定义区域 $\#030Ch$ 管理的服务区域提供服务时,它在图 18 所示区域中间密钥 K_c 的基础上加密存储在服务定义区域 $\#030Ch$ 中的服务密钥 $\#030Ch$ 以产生服务中间密钥 $K_{\#030Ch}$, 并将该密钥与所述区域中间密钥 K_c 一起登录到服务提供机 111 中。管理者 C 还将位于它的所述区域定义区域 $\#0300h$ 的层的上面的较上层的区域定义区域的区域码、即,在这种情况下,是管理者 A 的区域定义区域 $\#0000h$ 的区域码 $\#0000h$ 、管理者 B1 的区域定义区域 $\#0100h$ 的区域码 $\#0100h$ 、它的区域定义区域 $\#0300h$ 的区域码 $\#0300h$ 以及在区域定义区域 $\#0300h$ 的层中形成的服务定义区域 $\#030Ch$ 的服务码 $\#030Ch$ 登录到服务提供机 111 中。

在这种情况下,当 IC 卡 2 被插入到服务提供机 111 中时,在服务提供机 111 和 IC 卡 2 之间执行随后的相互确认。

即,如图 19 所示,已登录的区域码 $\#0000h$ 、 $\#0100h$ 和 $\#0300h$ 以

及服务码 # 030Ch 被传送给 IC 卡 2。在 IC 卡 2(定序器 91)中, 从服务提供机 111 中接收区域码 # 0000h、# 0100h 和 # 0300h 以及服务码 # 030Ch。

在 IC 卡 2 中, 读出存储在系统定义块(图 6)中的系统密钥, 并从具有从服务提供机 111 接收的区域码 # 0000h、# 0100h 或 # 0300h 的区域定义区域中读出区域密钥 # 0000h、# 0100h 或 0300h。另外, 在区域密钥 # 0000h 的基础上加密所述系统密钥, 以便产生与所述区域中间密钥 K_A 相同的密钥。在区域密钥 # 0100h 的基础上加密与所述区域中间密钥 K_A 相同的密钥, 以便产生与区域中间密钥 K_{B1} 相同的密钥。在区域密钥 # 0300h 的基础上加密与区域中间密钥 K_{B1} 相同的密钥, 以便产生被登录在图 18 的服务提供机 111 中的区域中间密钥 K_C 相同的密钥。与所述区域中间密钥 K_C 相同的密钥被设置为用于确认的第一访问密钥 K_{bc} 。

在 IC 卡 2 中, 从具有从服务提供机 111 中接收的服务码 # 030Ch 的服务定义区域读出服务密钥 # 030Ch。在所述服务密钥 # 030Ch 的基础上加密所述区域中间密钥 K_C , 借此以产生与登录在图 18 所示服务提供机 111 中的所述服务中间密钥 $K_{#030Ch}$ 相同的密钥。与所述服务中间密钥 $K_{#030Ch}$ 相同的密钥被设置为用于确认的第二访问密钥 K_{ac} 。

因此, 在上述情况下, 是所述第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的区域中间密钥 K_C 或服务中间密钥 $K_{#030Ch}$ 被登录到服务提供机 111 中, 和在 IC 卡 2 中产生是所述第一访问密钥 K_{bc} 或第二访问密钥 K_{ac} 的区域中间密钥 K_C 或服务中间密钥 $K_{#030Ch}$ 。

和在结合图 14 和 15 所描述的情况相同, 在 IC 卡 2 和服务提供机 111 之间执行相互确认。

作为所述相互确认的结果, 如果 IC 卡 2 和服务提供机 111 都被识别为是合适的, 则在 IC 卡 2 中允许仅对由具有从服务提供机 111 传送的服务码的服务定义区域管理的服务区域进行访问。因此, 在图 18 和 19 的情况下, 可以仅对由服务定义区域 # 030Ch 管理的服务区域进行访问。

即, 知道所述区域中间密钥 K_C 、所述区域码 # 0000h、# 0100h、# 0300h、所述服务密钥 # 030Ch 和服务码 # 030Ch 的管理者 C 能够对由服务定义区域 # 030Ch 管理的服务区域进行访问。但是, 管理者 C 既不知道服务密钥 # 0008h 也不知道服务密钥 # 1022h, 所以, 它基本上不能访问由服务定义区域 # 0008h 或 # 1022h 管理的服务区域。

如上所述,即使当所述管理者不知道较上层的区域密钥时,它也能够访问它的服务区域。

如上所述,每个管理者都不能访问由该管理者不知道所述服务密钥的服务定义区域管理的任何服务区域。但是,例如,存在管理者 C 不仅希望使用
5 由它的服务定义区域 # 030Ch 管理的服务区域执行服务、并且希望使用由管理者 B 的服务定义区域 # 1022h 管理的服务区域执行服务的情况。

在这种情况下,为了使管理者 C 得以访问由服务定义区域 # 1022h 管理的
10 的服务区域,管理者 C 必须知道结合图 16 和 17 所描述的所述区域中间密钥 K_{B2} 、所述区域码 # 0000h、# 1000h、所述服务密钥 # 1022h 和所述服务码 # 1022h。因此,必须从管理者 B2 得到这些信息。

但是,管理者 B2 所知道的服务密钥 # 1022h 即使是作为管理者 B2 的母层的管理者 A 所不知道的,因此,从安全角度来看,仅被允许管理者 B2 知道的服务密钥 # 1022h 被告知管理者 C 是很不利的。

在这种情况下,即使当忽略所述安全问题时,为了使管理者 C 得以访问
15 分别由服务定义区域 # 030Ch 或 # 1022 管理的两个服务区域,在 IC 卡 2 中必须执行图 17 所示的处理以产生用于对由服务定义区域 # 030Ch 管理的
服务区域进行访问的第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 并执行相互确认,还要执行图 19 所示的处理以产生用于对由服务定义区域 # 1022h 管理的
服务区域进行访问的第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 并执行相互确认。

20 因此,当在每个服务区域执行用于对一个服务区域进行访问的相互确认时,对所述服务区域进行快速访问是困难的。结果是当图 3 所示的卡系统被
应用于在火车站检查车票时,对 IC 卡 2 的预定服务区域的访问以及在其中经常往返者经过在检票口处设置的门这个相对短的时间周期内写入或读出数据
是非常困难的。

25 因此,在管理者 C 不仅使用由它的服务定义区域 # 030Ch 管理的
服务区域提供服务、而且使用由管理者 B2 的服务定义区域 # 1022h 管理的
服务区域提供服务的情况下,为了解决安全问题和保证对所述服务区域的快速访问,在管理者 C 和 B2 之间执行图 20 所示的信息传送并将所述信息登录到
服务提供机 111 中。

30 即,管理者 C 在区域中间密钥 K_c 的基础上与图 18 所示情况相同地加密
存储在服务定义区域 # 030Ch 中的服务密钥 # 030Ch 以产生服务中间密钥 K

030Ch。另外，管理者 C 向管理者 B2 传送所述服务中间密钥 $K_{\#030Ch}$ 并在服务密钥 # 1022h 的基础上加密它。管理者 C 接收作为在服务密钥 # 1022h 基础上对服务中间密钥 $K_{\#030Ch}$ 加密结果的服务中间密钥 $K_{\#1022h}$ 和服务码 # 1022h。

- 5 因此，在管理者 C 和管理者 B2 之间只传送服务中间密钥 $K_{\#030Ch}$ 和 $K_{\#1022h}$ ，既不存在只由管理者 C 知道的服务密钥 # 030Ch 被管理者 B2 知道的情况，也不存在只由管理者 B2 知道的服务密钥 # 1022h 被管理者 C 知道的情况。即，不存在安全问题。

- 从管理者 B2 接收服务中间密钥 $K_{\#1022h}$ 和服务码 # 1022h 的管理者 C
10 将位于它的区域定义区域 # 0300h 的层的上面的较上层中的区域定义区域的区域码、即在这种情况下是管理者 A 的区域定义区域 # 0000h 的区域码 # 0000h、管理者 B1 的区域定义区域 # 0100h 的区域码 # 0100h 和管理者 C 的区域定义区域 # 0300h 的区域码 # 0300h 登录到服务提供机 111 中。另外，管理者 C 将所述区域中间密钥 K_c 和在区域定义区域 # 0300h 的层中形成的
15 服务定义区域 # 030Ch 的服务码 # 030Ch 登录到服务提供机 111 中。

在这种情况下，当服务提供机 111 被插入到 IC 卡 2 中时，在所述服务提供机 111 和 IC 卡 2 之间执行随后的相互确认。

- 即，如图 21 所示，服务提供机 111 向 IC 卡 2 传送已登录的区域码 # 0000h、# 0100 和 # 0300h 以及服务码 # 030Ch 和 # 1022h。在 IC 卡 2(定
20 序器 91)中，接收来自服务提供机 111 的区域码 # 0000h、# 0100h 和 # 0300h 以及服务码 # 030Ch 和 # 1022h。

- 在 IC 卡 2 中，读出存储在所述系统定义块(图 6)中的系统密钥，和从具有从服务提供机 111 接收的区域码 # 0000、# 0100h 或 # 0300h 的区域定义区域中读出区域密钥 # 0000h、# 0100h 或 # 0300h，和与在图 19 所描述情
25 况相同地产生与登录在图 20 所示服务提供机 111 中的区域中间密钥 K_c 相同的密钥。与所述区域中间密钥 K_c 相同的密钥被设置为用于确认的第一访问密钥 K_{bc} 。

- 在 IC 卡 2 中，从分别具有从服务提供机 111 接收的服务码 # 030Ch 或 # 1022h 的服务定义区域中读出服务密钥 # 030Ch 或 # 1022h。在服务密钥 # 030Ch 的基础上加密所述区域中间密钥 K_c ，结果是产生与服务中间密钥 $K_{\#030Ch}$
30 $K_{\#030Ch}$ 相同的密钥。另外，在服务密钥 # 1022h 的基础上加密与服务中间密钥

$K_{\#030Ch}$ 相同的密钥, 和产生与登录在图 20 所示服务提供机 111 中的服务中间密钥 $K_{\#1022h}$ 相同的密钥。与所述服务中间密钥 $K_{\#1022h}$ 相同的密钥被设置为用于确认的第二访问密钥 K_{ac} 。

- 5 因此, 在上述情况中, 是所述第一访问密钥 K_{bc} 或所述第二访问密钥 K_{ac} 的区域中间密钥 K_c 或服务中间密钥 $K_{\#1022h}$ 被登录在所述服务提供机 111 中, 和在 IC 卡 2 中产生是所述第一访问密钥 k_{bc} 或所述第二访问密钥 K_{ac} 的区域中间密钥 K_c 或服务中间密钥 $K_{\#1022h}$ 。

与图 14 和 15 所示情况相同, 在 IC 卡 2 和服务提供机 111 中执行相互的确认。

- 10 作为相互确认的结果, 如果 IC 卡 2 和服务提供机 111 都被判断是合适的, 在 IC 卡 2 中允许仅对由具有从服务提供机 111 传送的服务码的服务定义区域管理的服务区域进行访问。因此, 在图 20 和 21 所示的情况下, 允许对由服务定义区域 $\#030Ch$ 管理的服务区域和由服务定义区域 $\#1022h$ 管理的服务区域进行访问。

- 15 如上所述, 通过在两个或更多个区域密钥或服务密钥的基础上加密所述系统密钥, 所述两个或更多个区域密钥或服务密钥被简化(组合)成第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 等两个密钥, 和使用所述第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 执行允许对由具有从服务提供机 111 传送的所述服务码的服务定义区域管理的服务区域进行访问的相互确认。因此, 即使当以访问多个
20 服务定义区域为目标时, 也能够短施加内完成所述相互确认, 由此保证对所述服务区的快速访问。

- 在图 14 和 15 的情况下, 使用所述第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 等两个密钥执行所述相互确认处理, 但是, 也可以例如只使用第二访问密钥 K_{ac} 执行所述相互确认处理。在这种情况下, 在 IC 卡 2 中, 通过在两个或更
25 多个区域密钥或服务密钥的基础上加密所述系统密钥, 所述两个或更多个区域密钥或服务密钥被简化成一个第二访问密钥 K_{ac} 。

- 另外, 如图 22 所示, 例如可以在被存储在所述制造 ID 块中并且是赋予 IC 卡 2 的一个固有值的制造 ID 的基础上, 使用通过加密所述第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 获得的加密结果。这里, 在图 22 中, 关于所述第一
30 访问密钥 K_{bc} , 通过对所述第一访问密钥 K_{bc} 和所述制造 ID 进行 EXOR 处理执行加密。关于第二访问密钥 K_{ac} , 执行以 DES 系统为基础的加密。关于第

二访问密钥 K_{ac} ，可以使用对所述第一访问密钥 K_{bc} 和所述制造 ID 执行 EXOR 的结果执行在所述 DES 系统基础上的加密。

如上所述，当加密所述第一访问密钥 K_{bc} 和第二访问密钥 K_{ac} 所获得的加密结果被用于相互确认时，能够更加增强安全性。在这种情况下，在服务提供机 111 中需要所述制造 ID，和它可以被从 IC 卡 2 传送。

接着，EEPROM 66 的存储区域具有一个其中区域定义区域被分层的分层结构，和每个区域定义区域和服务定义区域被指定存储用于确认的区域密钥和服务密钥。结果是，可以灵活地执行随后的访问控制。

即，当一个管理者被用做母层管理者和由于被分配了所述母层管理者的资源的子层管理者进行了不正当的服务而希望停止由所述子层管理者提供的服务时，所述母层管理者可以通过改变存储在所述区域定义区域中的所述区域密钥禁止所述子层管理者访问 IC 卡 2。

具体地说，例如当管理者 B1 停止图 7 所示管理者 C 的提供服务时，管理者 B1 改变存储在 IC 卡 2 的区域定义区域 # 0100h 中的区域密钥 # 0100h。在这种情况下，在图 19 中也改变在 IC 卡 2 中形成的区域中间密钥 K_{B1} 、以及区域中间密钥 K_c ，这样，只知道改变以前的区域中间密钥 K_c 的管理者 C 就不能访问服务定义区域 # 030Ch。

是管理者 C 的母层管理者的管理者 B1 的母层管理者的管理者 A 可以改变存储在区域定义区域 # 0000h 中的区域密钥 # 0000h 以禁止对服务定义区域 # 030Ch 进行访问。但是，在这种情况下，是管理者 A 的子层的管理者 B2 不能访问由管理者 B2 的服务定义区域 # 1022h 管理的服务区域。即，当一个管理者改变它的区域密钥时，不能对在与所述区域密钥对应的区域定义区域的层(子层、孙子层)中的由区域定义区域管理的服务定义区域进行访问。

在图 20 和 21 中，管理者 C 使用(由)为管理者 B2 共用的管理者 B2 的服务定义区域 # 1022h(管理的服务区域)。但是，对于某些类型的密钥管理来讲在管理者之间所述服务定义区域的更加复杂的共用是也可能。

具体地说，例如，假设在 EEPROM 66 中构成图 23 所示的层结构。即，在图 23 中，作为用做 IC 卡 2 发行者的管理者 A 的区域定义区域 # 0000h 的所述层的子层，形成管理者 E 的区域定义区域 # 5000h 和管理者 G 的区域定义区域 # 7000h。另外，在管理者 E 的区域定义区域 # 5000h 的层中形成服

务定义区域# 5008h、# 5048h、# 5088h和# 50C8h，和形成管理者F的区域定义区域# 6000h。

再有，在管理者F的区域定义区域# 6000h的层中形成服务定义区域# 6008h和# 6048h，和在管理者G的区域定义区域# 7000h的层中形成服务定义区域# 7008h和# 70C8h。

在上述的层结构中，管理者A在图24的(A)所示区域密钥# 0000h的基础上加密所述系统密钥，和将所述加密结果传送给用做子层管理者的管理者E和G。

如图24的(B)所示，在区域密钥# 5000h的基础上，管理者E对在来自管理者A的区域密钥# 0000h基础上对所述系统密钥进行加密的加密结果进行加密，和使用所述加密结果作为第一访问密钥 K_{E1} 。另外，管理者E在服务密钥# 5008h、# 5048h、# 5088h和50C8h中每一个的基础上陆续加密所述第一访问密钥 K_{E1} (在区域密钥# 5000h基础上的加密结果)，和使用最终的加密结果作为第二访问密钥 K_{E2} 。

如图24的(C)所示，管理者F被提供有来自管理者E的所述第一访问密钥 K_{E1} (在区域密钥# 5000h基础上的加密结果)，和在区域密钥# 6000h的基础上对其加密，并将所述加密结果设置为第一访问密钥 K_{F1} 。另外，管理者F在服务密钥# 6008h和# 6048h中每一个的基础上加密所述第一访问密钥 K_{F1} (在区域密钥# 6000h基础上的加密结果)，并将所述加密结果传送给管理者E以在服务密钥# 5048h和# 5088h中每一个的基础上陆续对其进行加密。此后，管理者F被提供有来自管理者E的所述加密结果并将它传送给管理者G以在服务密钥# 70C8h的基础上对其加密。管理者F被提供有来自管理者G的加密结果，和使用它作为第二访问密钥 K_{F2} 。

如图24的(D)所示，管理者G在区域密钥# 7000h的基础上，对在来自管理者A的区域密钥# 0000h的基础上对所述系统密钥的加密结果进行加密，和使用所述加密结果作为第一访问密钥 K_{G1} 。另外，管理者G在服务密钥# 7008h和# 70C8h中每一个的基础上陆续加密所述第一访问密钥 K_{G1} (在区域密钥# 7000h基础上的加密结果)，和将最终加密结果传送给管理者F以在服务密钥# 6048h的基础上对其加密。此后，管理者G将管理者F使用服务密钥# 6048h的加密结果传送给管理者E，以在服务密钥# 5088h和# 50C8h中每一个的基础上陆续加密所述加密结果。管理者G被提供有来自管

理者 E 的加密结果和使用它作为第二访问密钥 K_{G2} 。

在这种情况下，在 IC 卡 2 中，根据图 24 所示情况相同的处理，使用存储在 EEPROM 66 中的所述区域密钥和服务密钥加密所述系统密钥，以产生第一访问密钥和第二访问密钥，借此，在管理者 E、F 和 G 中能够相互进行图 5 25 所示服务定义区域的共同使用。

即，管理者 E 只能访问它的服务定义区域 # 5008h、# 5048h、# 5088h 和 50C8h。管理者 F 不仅能够访问它的服务定义区域 # 6008h 和 # 6048h，还能够访问管理者 E 的服务定义区域 # 5048h 和 # 5088h 以及管理者 G 的服务定义区域 # 70C8h。管理者 G 不仅能够访问它的服务定义区域 # 7008h 和 10 # 70C8h，还能够访问管理者 E 的服务定义区域 # 5088h 和 # 50C8h 以及管理者 F 的服务定义区域 # 6048h。

在图 24 所示的密钥传送中，不存在一个管理者的所述服务密钥被另一个管理者知道的情况。即，管理者 E 的服务密钥 # 5008h、# 5048h、# 5088h 和 # 50C8h 不仅决不会被母层管理者 A 知道，也决不会被管理者 F 和 G 知 15 道。类似的，管理者 F 的服务密钥 # 6008h 和 # 6048h 决不会被管理者 E 和 G 知道，和管理者 G 的服务密钥 # 7008h 和 # 70C8h 决不会被管理者 E 和 F 知道。

另外，如上所述，当某个管理者改变它的服务密钥时，不可能对由在所述区域定义区域的层中层的区域定义区域管理的所有服务定义区域进行访问。即，当母层管理者改变所述区域密钥时，子层管理者不能访问 IC 卡 2。但是，根据一个特殊的密钥管理方法，能够禁止一个特殊的子层管理者的访问。

具体地说，例如，假设在 EEPROM 66 中构成图 26 所示的层结构。即，在图 26 中，管理者 H 的区域定义区域 # 8000h、管理者 I 的区域定义区域 # 25 9000h 和管理者 J 的区域定义区域 # A000h 被形成为用做 IC 卡 2 的发行者的管理者 A 的区域定义区域 # 0000h 的层的子层。另外，在管理者 H 的区域定义区域 # 8000h 的层中形成服务定义区域 # 8008h、# 8104h 和 # 8105h。

在上述的层结构中，如图 27 的(A)所示，管理者 A 在区域密钥 # 0000h 的基础上加密所述系统密钥和将加密结果传送给用做它的子层管理者的管理 30 者 I 和 J。

如图 27 的(C)所示，管理者 I 在区域密钥 # 9000h 的基础上加密以来自

管理者 A 的区域密钥 # 0000h 为基础对所述系统密钥加密的加密结果, 并使用所述加密结果作为第一访问密钥 K_{J1} 。另外, 管理者 I 向管理者 H 传送所述第一访问密钥 K_{J1} (在区域密钥 # 9000h 基础上的加密结果)以在图 27 的(B)所示服务密钥 # 8008h 和 # 8104h 中每一个的基础上陆续加密它。然后, 管理者 I 使用所述加密结果作为如图 27 的(C)所示的第二访问密钥 K_{J2} 。

如图 27 的(D)所示, 管理者 J 在区域密钥 # A000h 的基础上加密以来自管理者 A 的区域密钥 # 0000h 为基础对所述系统密钥加密的加密结果, 并使用所述加密结果作为第一访问密钥 K_{J1} 。另外, 管理者 J 向管理者 H 传送所述第一访问密钥 K_{J1} (在区域密钥 # A000h 基础上的加密结果)以在图 27 的(B)所示服务密钥 # 8008h 和 # 8105h 中每一个的基础上陆续加密所述加密结果。管理者 J 使用所述加密结果作为图 27(D)所示的第二访问密钥 K_{J2} 。

在这种情况下, 在 IC 卡 2 中, 根据图 27 所示的相同处理使用存储在 EEPROM 66 中的所述区域密钥和服务密钥加密所述系统密钥以产生所述第一访问密钥和第二访问密钥, 借此, 管理者 I 能够访问管理者 H 的服务定义区域 # 8008h 和 # 8104h 和管理者 J 能够访问管理者 H 的服务定义区域 # 8008h 和 # 8105h。

管理者 H 形成所述服务定义区域 # 8008h 以便在管理者 I 和 J 之间共同使用它的数据, 形成服务定义区域 # 8104h 或 # 8105h 作为所谓虚服务定义区域, 以便对由管理者 I 或管理者 J 中的每一个对所述服务定义区域 # 8008h 的访问进行控制。因此, 不需要由所述服务定义区域 # 8104h 和 # 8105h 管理的服务区域, 并且它的容量可以等于零。

在这种情况下, 例如当管理者 H 改变服务密钥 # 8104h 时, 其中使用服务密钥 # 8104h 产生所述第二访问密钥 K_{J2} 以在 IC 卡 2 中执行所述确认处理的管理者 I 不能访问服务定义区域 # 8008h。即, 只禁止管理者 I 对服务定义区域 # 8008h 进行访问。相反, 例如, 当管理者 H 改变所述服务密钥 # 8105h 时, 其中使用服务密钥 # 8105h 产生所述第二访问密钥 K_{J2} 以在 IC 卡 2 中执行确认处理的管理者 J 不能访问所述服务定义区域 # 8008h。即, 只禁止管理者 J 访问所述服务定义区域 # 8008h。

如上所述, 可以禁止特殊的子层管理者使用虚服务定义区域进行访问。接着, 在用于管理诸如代码范围、分配块数、区域密钥、服务密钥等所述管理者形成结合图 8 所述的区域定义区域和服务定义区域所需的用户块的

管理信息(此后称之为已登录卡的发行信息)被登录在已登录卡的发卡机 101 中的情况下, 当所述已登录卡的发卡机 111 被设置在火车站、零售店或其它非安全场所中和执行已登录卡的发行工作时, 执行诸如分流、篡改等不正当实践的概率是很高的, 因此, 在安全管理方面是很不利的。

- 5 因此, 在这种情况下, 如图 28 所示, 要形成区域定义区域和服务定义区域的管理者(此后称之为已登录卡的发行经营者)加密所述已登录卡的发行信息, 并将加密后的卡的发行信息经过诸如公用线、国际互联网、地波、卫星线、CATV(有线电视)网络等的传送媒体 121 传送给已登录卡的发卡机 101 以将所述信息登录到已登录卡的发卡机 101 中。在已登录卡的发卡机 101 中, 加密后的已登录卡的发行信息被传送给 IC 卡 2, 和在 IC 卡 2 中, 加密后的已登录卡的发行信息被译码以形成所述区域定义区域和服务定义区域。

这里, 图 28 示出了一种状态(执行已登录卡的发行工作的状态), 在这种状态下, 在其中仅构成了用于由管理者 # 1 提供服务的一个存储区域的 IC 卡 2 中, 如上所述地构成了用于由管理者 # 2 提供服务的一个存储区域。

- 15 接着, 图 29 示出了用于执行上述已登录卡的发行工作的已登录卡的发行处理系统的一个实施例的结构。

- 已登录卡的发行信息提供装置 131 通过执行下面将要描述的已登录卡的发行信息提供处理, 经过一个传送媒体 121 向所述已登录卡的发卡机 101 传送已登录卡的发行信息(此后称之为加密后的已登录卡的发行信息)。已登录卡的发卡机 101 从已登录卡的发行信息提供装置 131 接收并登录所述加密后的已登录卡的发行信息。当 IC 卡 2 被插入到所述已登录卡的发卡机 101 中时, 已登录卡的发卡机 101 将加密后的已登录卡的发行信息传送给 IC 卡 2。IC 卡 2 从已登录卡的发卡机 101 中接收所述加密后的已登录卡的发行信息并执行下面将要描述的译码处理, 以将所述加密后的已登录卡的发行信息译码成原来的已登录卡的发行信息。此后, IC 卡 2 在译码后的已登录卡的发行信息的基础上执行上述区域形成处理(图 9)或服务形成处理(图 10)以形成所述区域定义区域或所述服务定义区域。

下面将结合图 30 的流程描述由所述已登录卡的发行信息提供装置 131 执行的已登录卡的发行信息提供处理。

- 30 所述已登录卡的发行信息提供装置 131 被提供有形成一个区域定义区域或服务码所需的代码范围、分配块数和区域密钥和形成一个服务定义区域所

需的分配块数和服务密钥。在步骤 S21 中，在这些输入信息的基础上形成所述已登录卡的发行信息。

- 即，当输入形成所述区域定义区域所需的代码范围、分配块数和区域密钥时，这些数据彼此关联以形成所述已登录卡的发行信息。当输入形成所述
- 5 服务定义区域所需的分配块数和服务密钥时，这些数据彼此关联地形成所述已登录卡的发行信息。

所述处理前进到步骤 S22，以运行用于在步骤 S21 中形成的已登录卡的发行信息的一个纠错码，和所述运行结果被用做用于检查篡改的检查码包含在已登录卡的发行信息中。

- 10 此后，在步骤 S23 加密已登录卡的发行信息。即，在步骤 S23 中，在要被在已登录的发行信息的基础上形成的区域定义区域或服务定义区域的母层的所述区域定义区域的区域密钥的基础上，加密已登录卡的发行信息，和它被设置为加密后的已登录卡的发行信息。

- 15 此后，所述处理前进到步骤 S24，在这里将一个识别码(当所述加密后的已登录卡的发行信息被用于形成一个区域定义区域时，所述识别码是所涉及的区域定义区域的区域码，和当它被用于形成一个服务定义区域时，所述识别码是它的服务码)作为一个标题添加到加密后的已登录卡的发行信息上，和所述识别码经过传送媒体 121 被传送给已登录卡的发卡机 101，在此之后完成所述已登录卡的发行信息的提供处理。

- 20 因此，例如，当母层管理者 A 形成图 7 所示子层管理者 B1 的区域定义区域 # 0100h 时，从所述已登录卡的发行信息提供装置 131 传送图 31 的(A)所示的加密后的已登录卡的发行信息。即，所述区域定义区域 # 0100h 的区域码 # 0100h 被作为标题设置在图 31 的(A)所示的加密后的已登录卡的发行信息的头部。由于区域码 # 0100h 被用于识别所述母层，所以，在 IC 卡 2
- 25 中，它没有被加密。另外，在已登录卡的发行信息提供装置 131 中，在输入信息的代码范围的基础上识别区域码 # 0100h。这是由于根据这个实施例，所述区域定义区域的代码范围的最小值被设置为区域码，因此，如上所述，可以在所述代码范围的基础上识别所述区域码。

- 30 要被存储在区域定义区域 # 0100h 中的从 # 0100h 到 # 03FFh 的代码范围、分配块数 33 和作为区域密钥 # 0100h 的 a0a0a0a0a0a0a0 以及检查码随后被陆续地加到所述未加密的区域码 # 0100h 作为标题。这些都是在用做

母层的所述区域定义区域# 0000h 的区域密钥# 0000h 的 0123456789abcdef 的基础上被加密的(如图 31(A)中阴影部分所示)。

当管理者 B2 形成图 7 所示它的服务定义区域# 1022h 时, 从已登录卡的发行信息提供装置 131 传送图 31(B)所示的加密后的已登录卡的发行信息。即, 服务定义区域# 1022h 的服务码# 1022h 被作为标题设置在图 31(B)所示加密后的已登录卡的发行信息的头部。由于服务码# 1022 被用于识别所述母层(所述服务定义区域所属于的层), 所以, 在 IC 卡 2 中它没有被加密。

要被存储在服务定义区域# 1022h 中的服务码# 1022h、分配块数 5、作为区域密钥# 1022h 的 0303030303030303 以及检查码随后被陆续地设置给未加密的服务码# 1022h 作为一个标题。这些都是在用做母层的区域定义区域# 1000h 的区域密钥# 1000h 的 c0c0c0c0c0c0c0c0 的基础上被加密的(图 31(B)中的阴影部分所示)。

由于已登录卡的发行信息被如上所述在所述母层的区域密钥的基础上被加密, 所以, 在已经知道它的区域密钥的情况下, 不能知道已登录卡的发行信息的内容。因此, 即使当如上所述加密后的已登录卡的发行信息被传递到一个不安全的场所时, 也可以避免其内容的泄露。结果是, 可以分布所述加密后的已登录卡的发行信息和请求第三方将该信息登录在已登录卡的发卡机 101 中或把它传送给 IC 卡 2。

在这种情况下, 已登录卡的发行信息被在所述母层的区域密钥的基础上进行加密, 这样, 对于在它的母层管理者的控制下执行已登录卡的发行信息提供处理是有利的。即, 当第三方执行所述已登录卡的发行信息提供处理时, 用于所述加密的所述母层管理者的区域密钥对于所述第三方必须是公开的, 和这在安全方面是很不利的。因此, 在所述母层管理者的控制下执行已登录卡的发行信息处理是有利的。

下面, 结合图 32 的流程描述由 IC 卡 2 执行的译码处理。

当如上所述从已登录卡的发行信息提供装置 131 传送加密后的已登录卡的发行信息时, 已登录卡的发卡机 101 接收和登录所述加密后的已登录卡的发行信息。当 IC 卡 2 被插入时, 已登录卡的发卡机 101 将加密后的已登录卡的发行信息传送给 IC 卡 2。IC 卡 2 从已登录卡的发卡机 101 接收加密后的已登录卡的发行信息以在步骤 S31 中在加密后的已登录卡的发行信息的基础上将所述区域定义区域识别为一个要被形成的区域定义区域或服务定义区域

的所述母层。

即，在步骤 S31 中，通过参考加密后的已登录卡的发行信息的标题，识别要被形成的所述区域定义区域或服务定义区域的区域码或服务码。在步骤 S31 中，从 EEPROM 66 中检测包含在所述代码范围中被如此识别的区域码或服务码的所述区域定义区域，和所述区域定义区域被识别为所述母层。

处理前进到步骤 S32 以在存储在在步骤 S31 中识别的所述母层的所述区域定义区域中的区域密钥的基础上译码所述加密后的已登录卡的发行信息，然后，处理前进到步骤 S33。在步骤 S33 中，在包含在译码后的已登录卡的发行信息中的所述检查码的基础上，判断所述已登录卡的发行信息是否已经被篡改。如果在步骤 S33 的判断结果是已登录卡的发行信息已经被篡改，处理前进到步骤 S34，以将指示所述已登录卡的发行信息已经被篡改的一个消息传送给已登录卡的发卡机 101，并执行丢弃译码后的已登录卡的发行信息等的差错处理，借此，完成译码处理。在这种情况下，所述译码处理被非正常结束，和没有形成所述区域定义区域或服务定义区域。

相反，如果在步骤 S33 的判断结果是所述已登录卡的发行信息没有被篡改，所述译码处理结束。在这种情况下，所述译码处理被正常结束，和执行将被如此译码的已登录卡的发行信息存储到 EEPROM 66 中的处理，即，形成所述区域定义区域或服务定义区域的区域形成处理(图 9)或服务形成处理(图 10)。

可以使用加密后的已登录卡的发行信息的标题代替检查码执行关于所述已登录卡的发行信息是否被篡改的检查。即，如果所述加密后的已登录卡的发行信息被用于形成所述区域定义区域，那么，所述区域码被如图 31(A)所示地设置在它的标题处，所述区域码可以和其后设置给所述区域码的加密后的代码范围的最小值相一致。因此，可以通过将设置在所述标题处的区域码和其后设置给所述区域码的代码范围的最小值进行比较来检查所述加密后的已登录卡的发行信息是否被篡改。另外，如果加密后的已登录卡的发行信息被用于形成所述服务定义区域，如图 31(B)所示，所述服务码被设置在所述标题处，和所述服务码可以和其后设置给所述服务码的加密后的服务码相一致。因此，可以通过将设置在所述标题处的服务码和其后设置给所述服务码的服务码进行比较，来检查所述加密后的已登录卡的发行信息是否被篡改。

如上所述,在所述已登录卡的发行信息提供装置 131 中,所述已登录卡的发行信息被加密以获得加密后的已登录卡的发行信息,和在 IC 卡 2 中译码加密后的已登录卡的发行信息。因此,即使当已登录卡的发卡机 101 被设置在一个不安全的地方并经过传送媒体 121 进行传送时,也可以避免诸如分流、篡改等不正当实践。

结果是,当执行已登录卡的发行工作以开始使用 IC 卡 2 提供新的服务时,不需要回收所述 IC 卡 2,因此可以减少回收所需的费用。另外,从 IC 卡 2 用户的角度看,当开始提供一个新的服务时,所述用户可以将 IC 卡 2 携带到设置有已登录卡的发卡机 101 的场所,并在不回收所述 IC 卡 2 的情况下执行已登录卡的发行工作,借此,所述用户可以被立即提供所述新的服务。

在前面的描述中,本发明被应用于一个非接触卡系统,在这种系统中,在非接触状态下执行所述通信。但是,本发明也可以被应用于一个卡系统,在这种卡系统中,在接触状态下执行所述通信。另外,本发明的应用范围并不局限于所述卡系统。

在这个实施例中,使用所谓的安全密钥系统执行所述确认,但是,也可以使用所谓的公开密钥系统执行所述确认。

在这个实施例中,当访问一个区域定义区域的层的服务定义区域时,通过在从所述区域定义区域的层到最上层的总线上连续使用所述区域定义区域的区域密钥产生所述第一访问密钥,但是,所述第一访问密钥的产生方法并不局限于上述方式。另外,根据这个实施例,通过连续使用要被访问的所述服务定义区域的服务密钥产生所述第二访问密钥。但是,所述第二访问密钥的产生方法并不局限于上述方式。即,可以通过连续使用任何两个或多个区域密钥或服务密钥产生所述第一访问密钥和第二访问密钥。

另外,在这个实施例中,所述用户块和系统块中的每一个都被存储在是一个存储器的 EEPROM 66 中。但是,所述用户块和系统块也可以被存储在物理上不同的存储器中。

在这个实施例中,数据被存储在 EEPROM 66 中,但是,所述数据也可以被存储在除 EEPROM 66 以外的半导体存储器、磁盘或类似的存储装置中。

在这个实施例中,在已登录卡的发行信息提供处理过程中,已登录卡的发行信息是在所述母层的区域定义区域的区域密钥的基础上被加密的。但

是，用于加密所述已登录卡的发行信息的密钥并不局限于所述母层的区域密钥。但是，由于需要译码加密后的已登录卡的发行信息，所以，用于加密已登录卡的发行信息的密钥必须被存储在 IC 卡 2 中。因此，当所述母层的区域密钥被用于加密已登录卡的发行信息时，所述母层的区域密钥已经被存储在 IC 卡 2 中，这样，除了所述母层的密钥之外，用于译码(加密)所述已登录卡的发行信息的密钥并不需要被存储在 IC 卡 2 中。

另外，在这个实施例中，在以层结构设计所述 EEPROM 66 的所述存储区域的同时对其进行管理。但是，本发明可以被应用于不以所述层结构管理所述 EEPROM 66 的存储区域的情况。

再有，在这个实施例中，加密后的已登录卡的发行信息被经过所述传送媒体 121 传送给已登录卡的发卡机 101 并被登录在所述已登录卡的发卡机 101 中。但是，所述加密后的已登录卡的发行信息也可以被存储在诸如磁盘、磁光盘、光盘、存储器卡、磁带等将被直接引入已登录卡的发卡机 101 中以登录所述加密后已登录卡的发行信息的记录媒体(存储媒体)中。

根据本发明第一方面的所述信息处理装置和本发明第二方面的所述信息处理方法，用于管理数据存储装置的存储区域和包含访问所述存储区域所需的一个密钥的管理信息被加密。因此，能够避免所述管理信息的内容被泄露给第三方。

根据本发明第三方面的所述信息处理装置和根据本发明第四方面的所述信息处理方法，用于管理数据存储装置的存储区域、包含访问所述存储区域所需的一个密钥并被加密的管理信息被译码。因此，可以避免所述管理信息的内容被泄露给第三方。

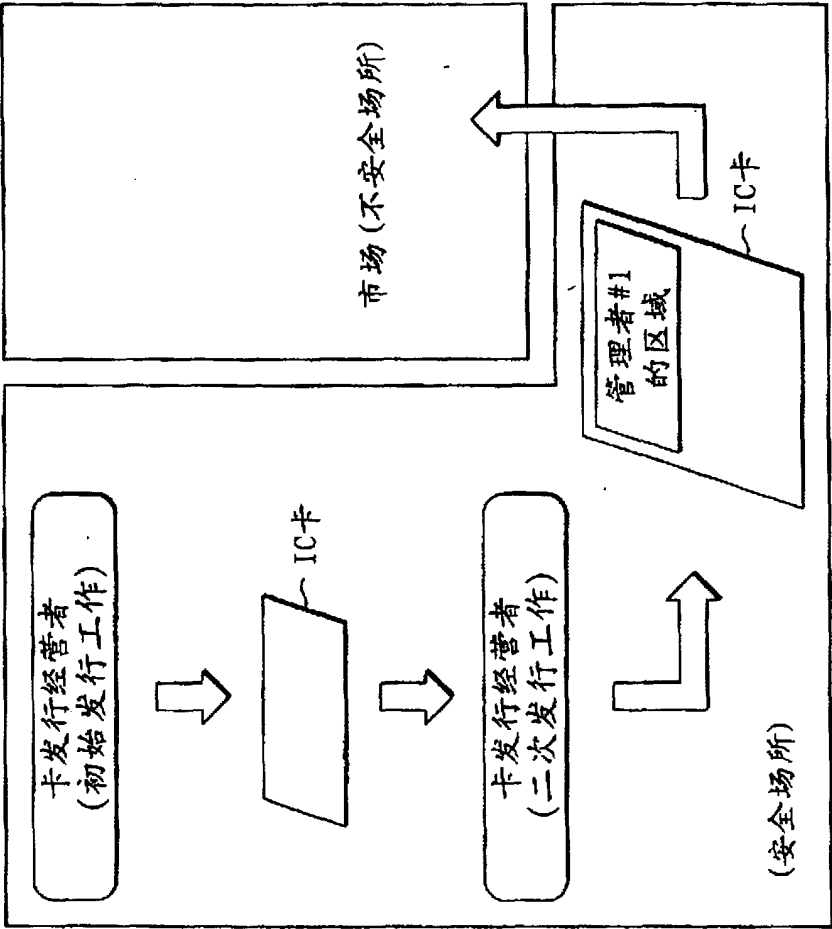


图 1

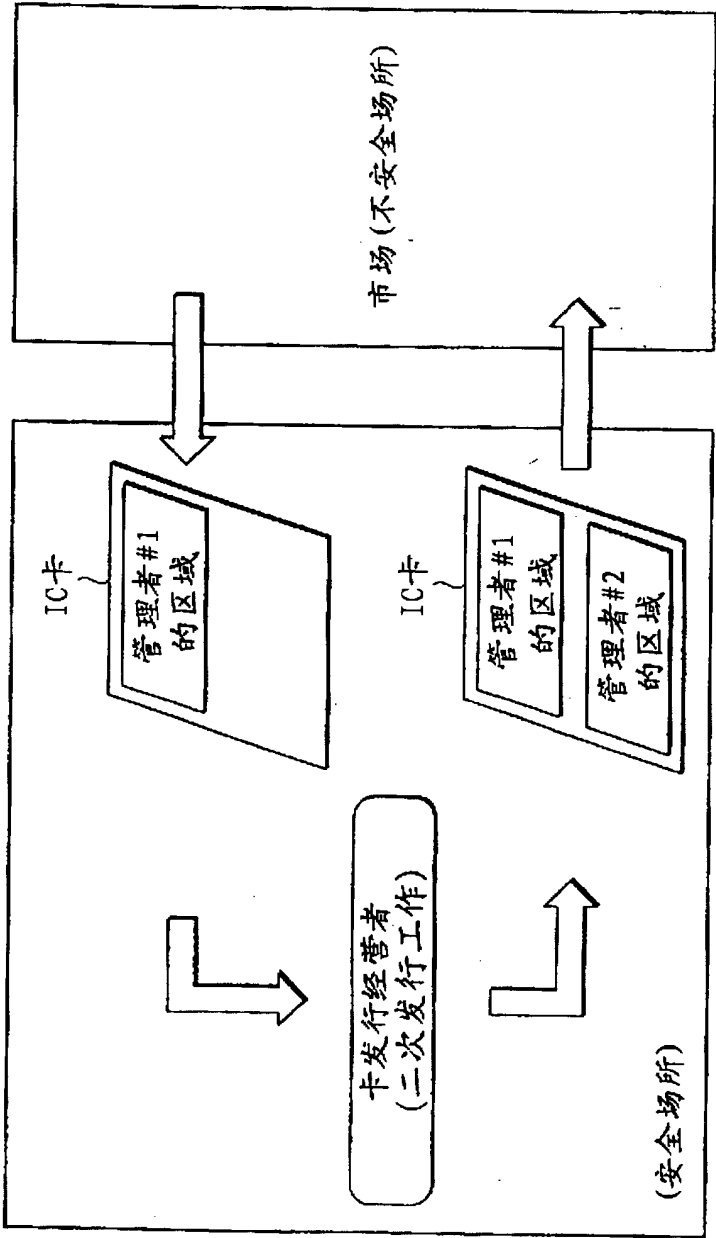


图 2

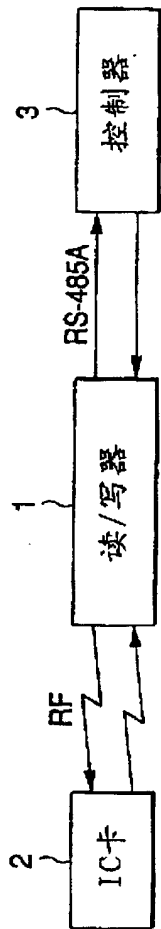


图 3

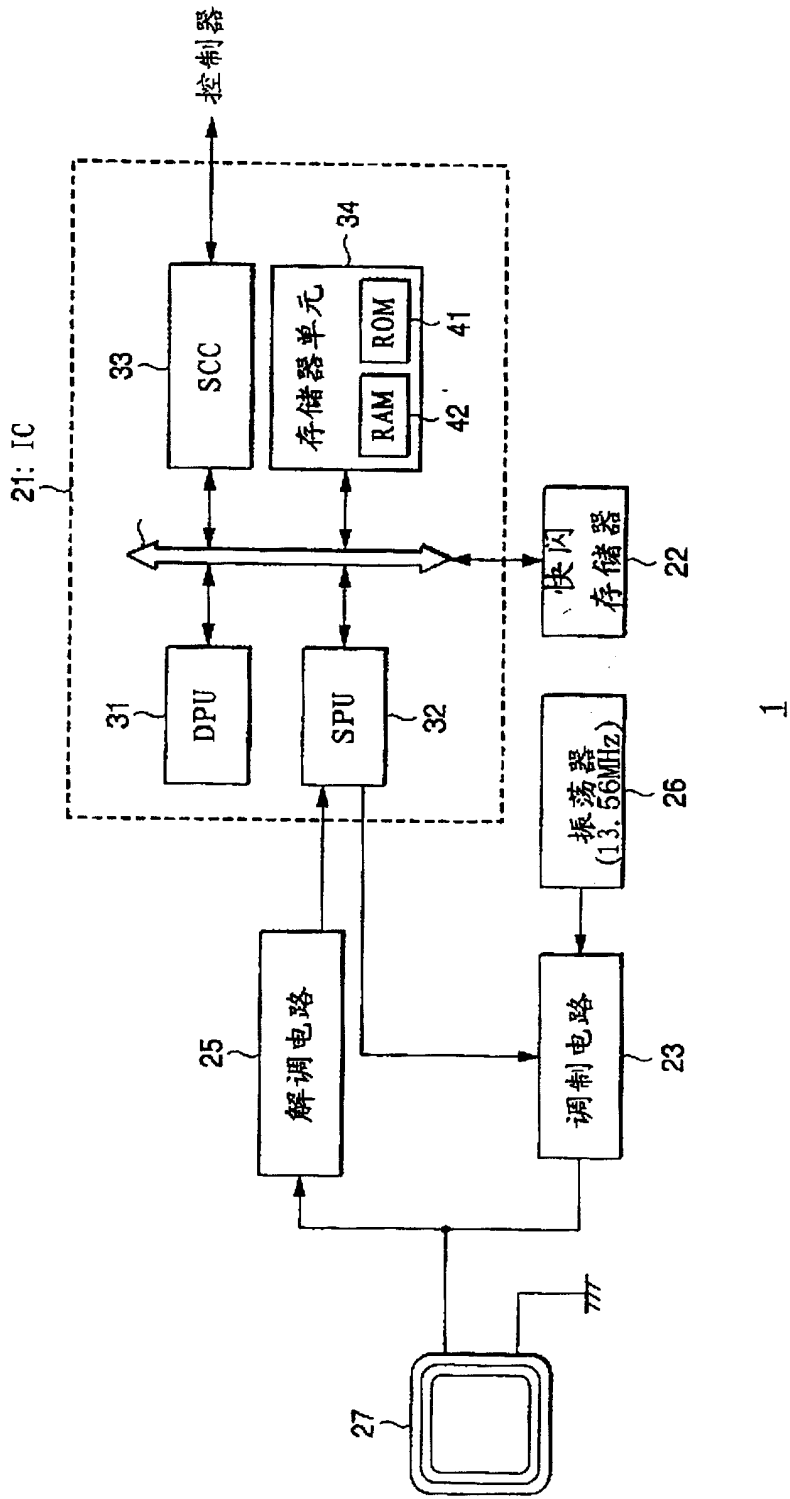
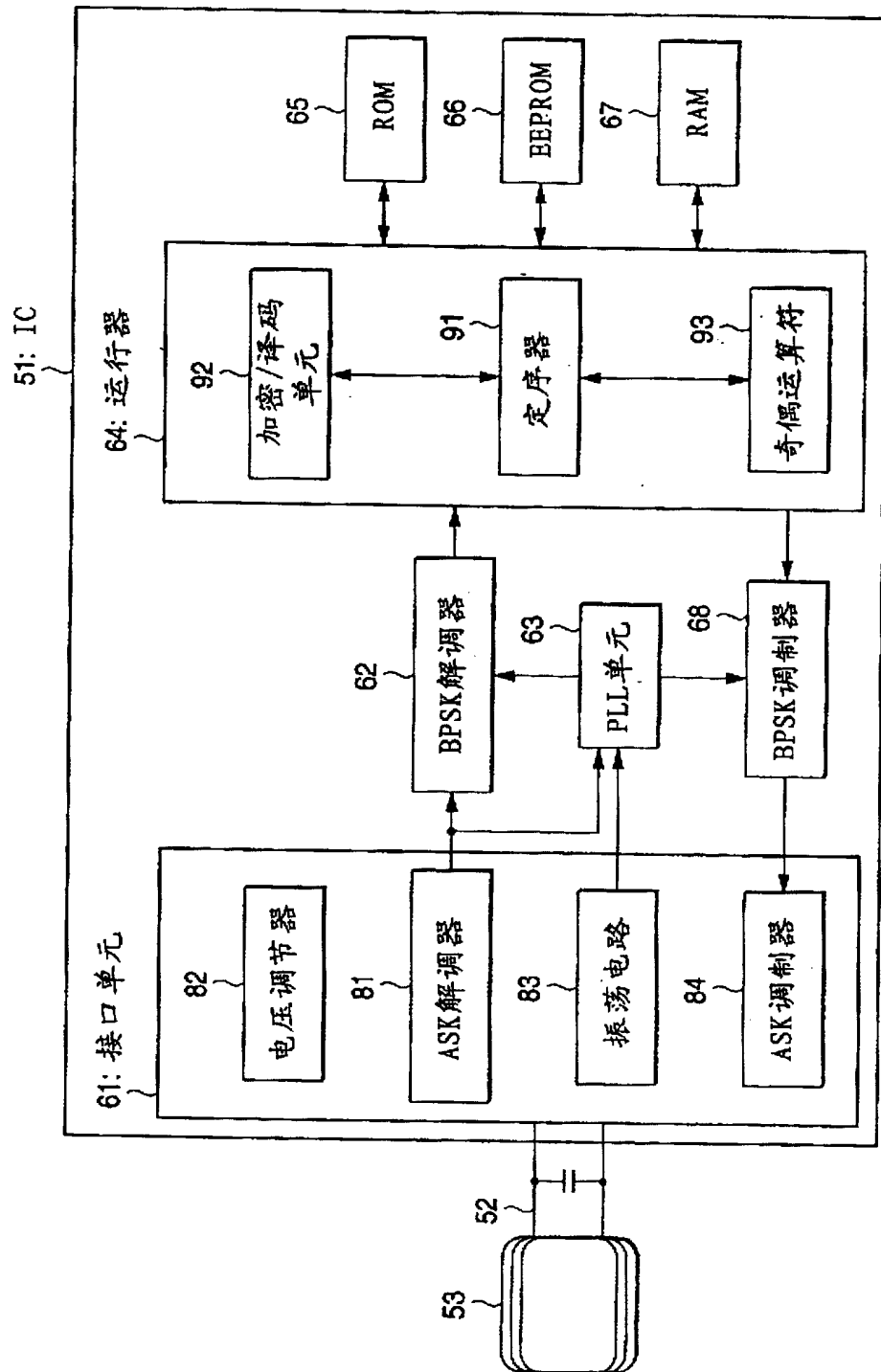


图 4



2

图 5

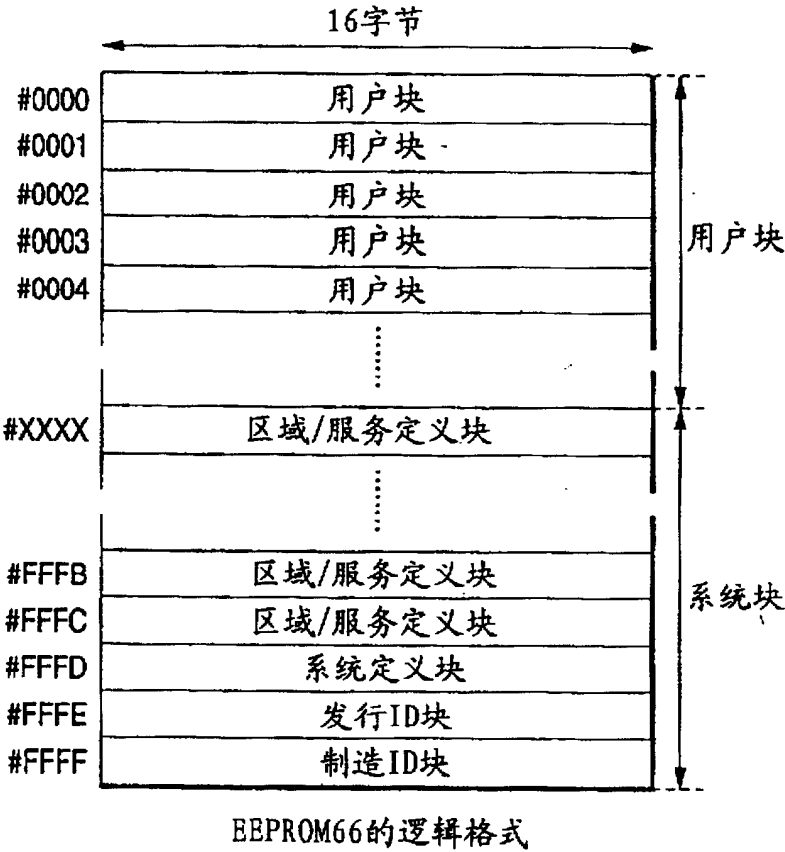
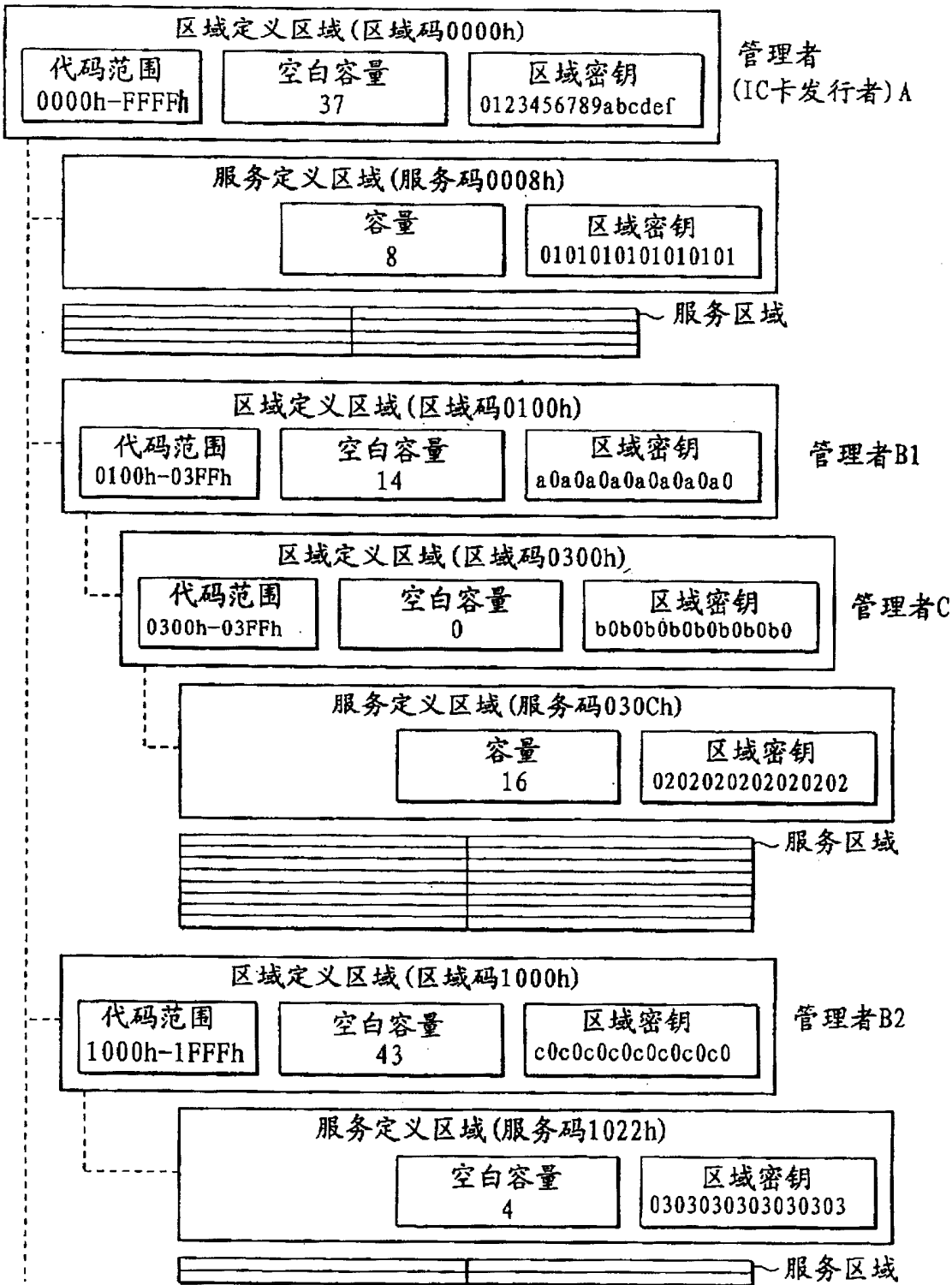


图 6



目录结构

图 7

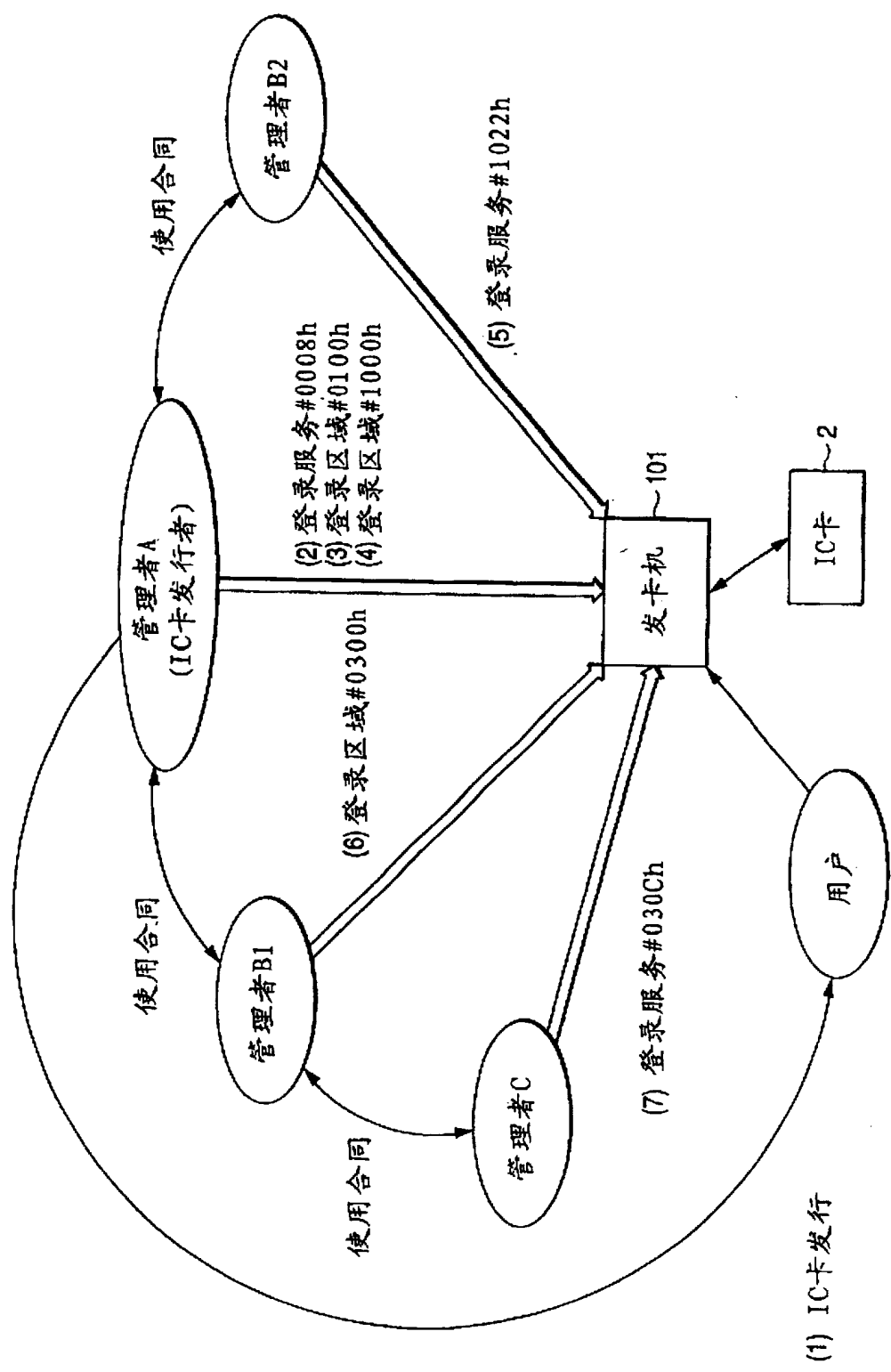


图 8

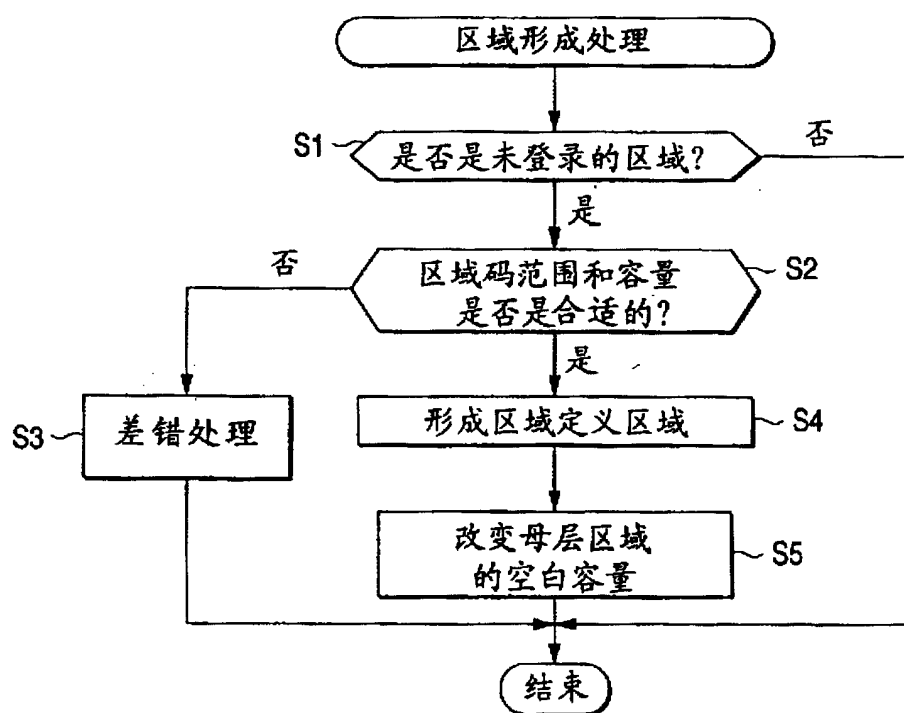


图 9

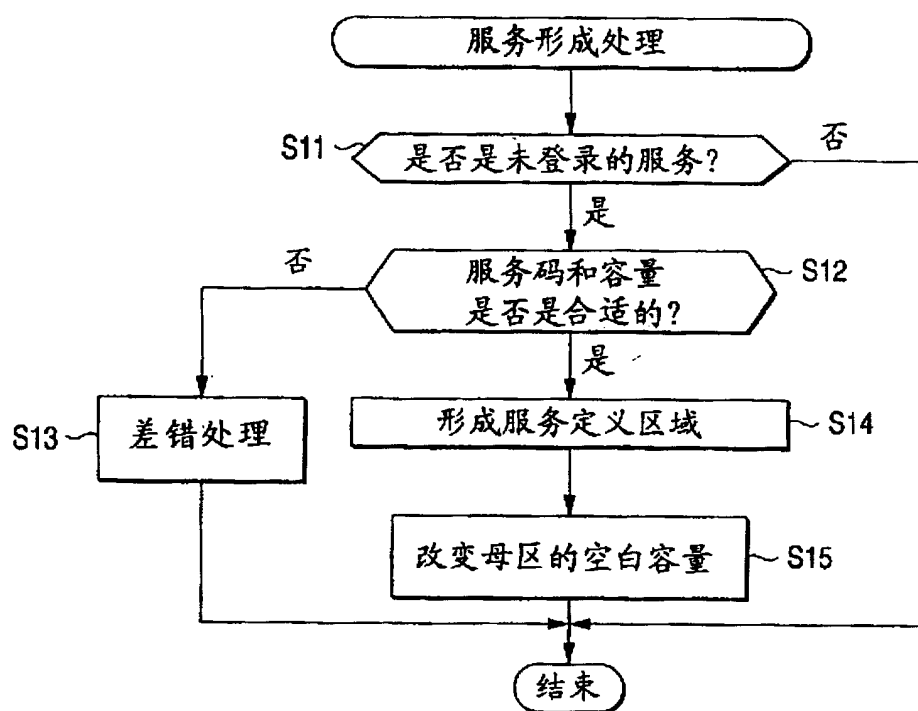


图 10

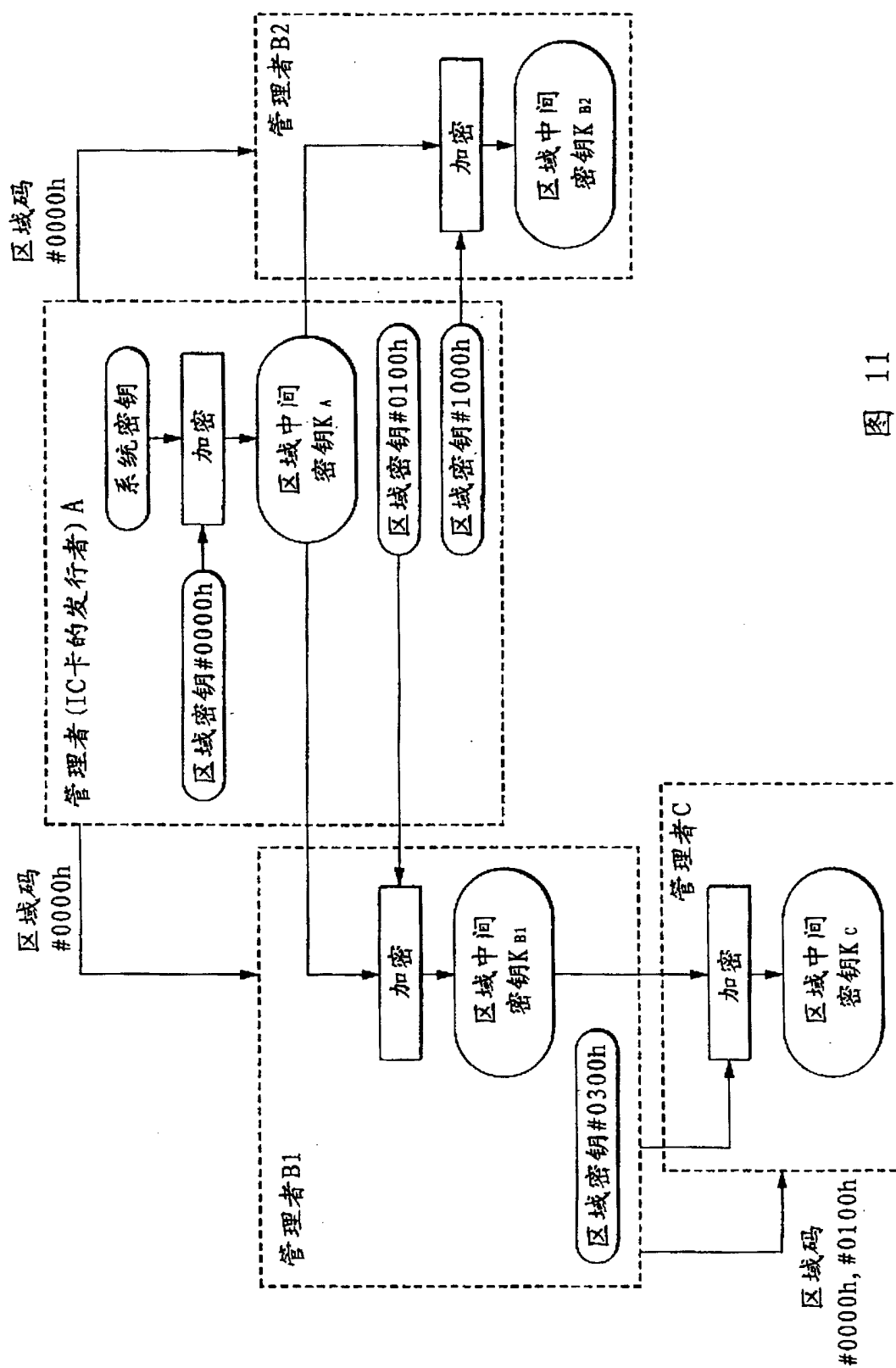


图 11

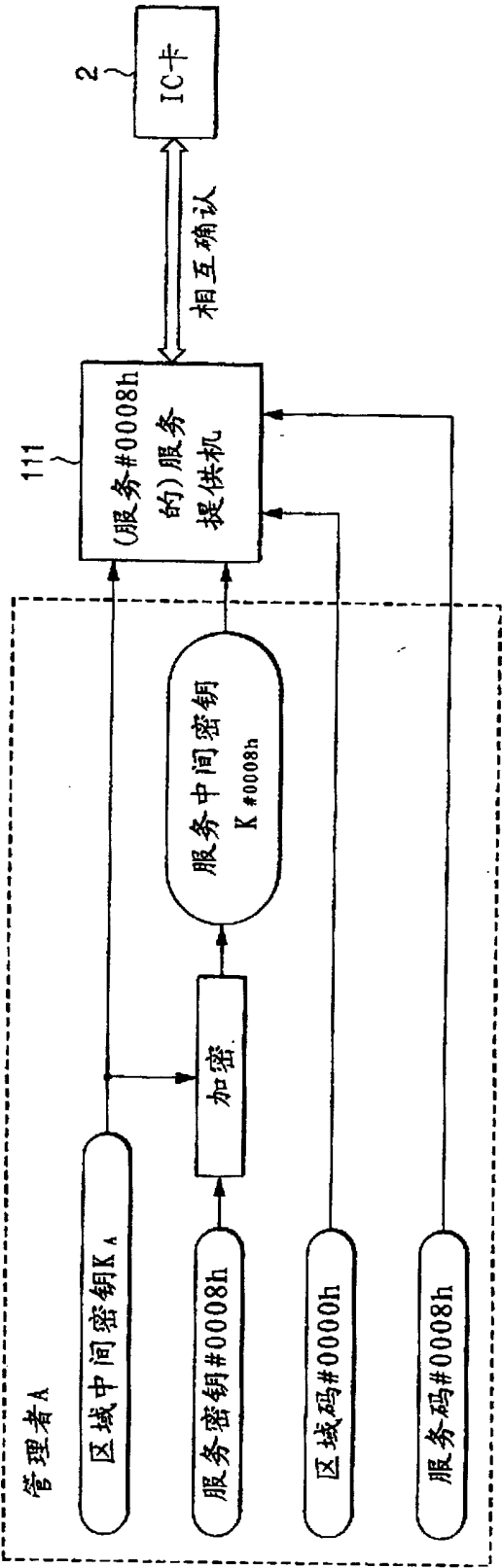


图 12

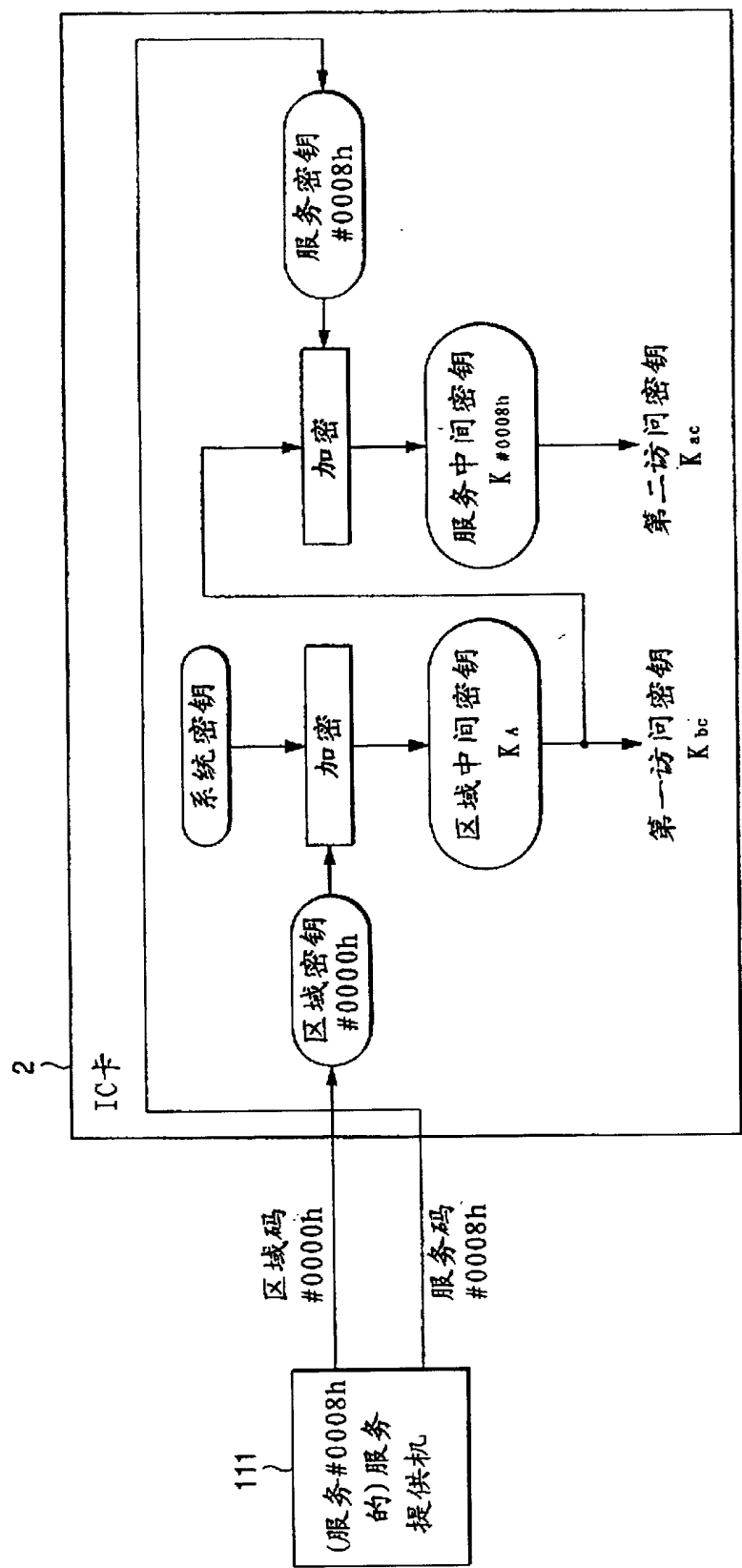


图 13

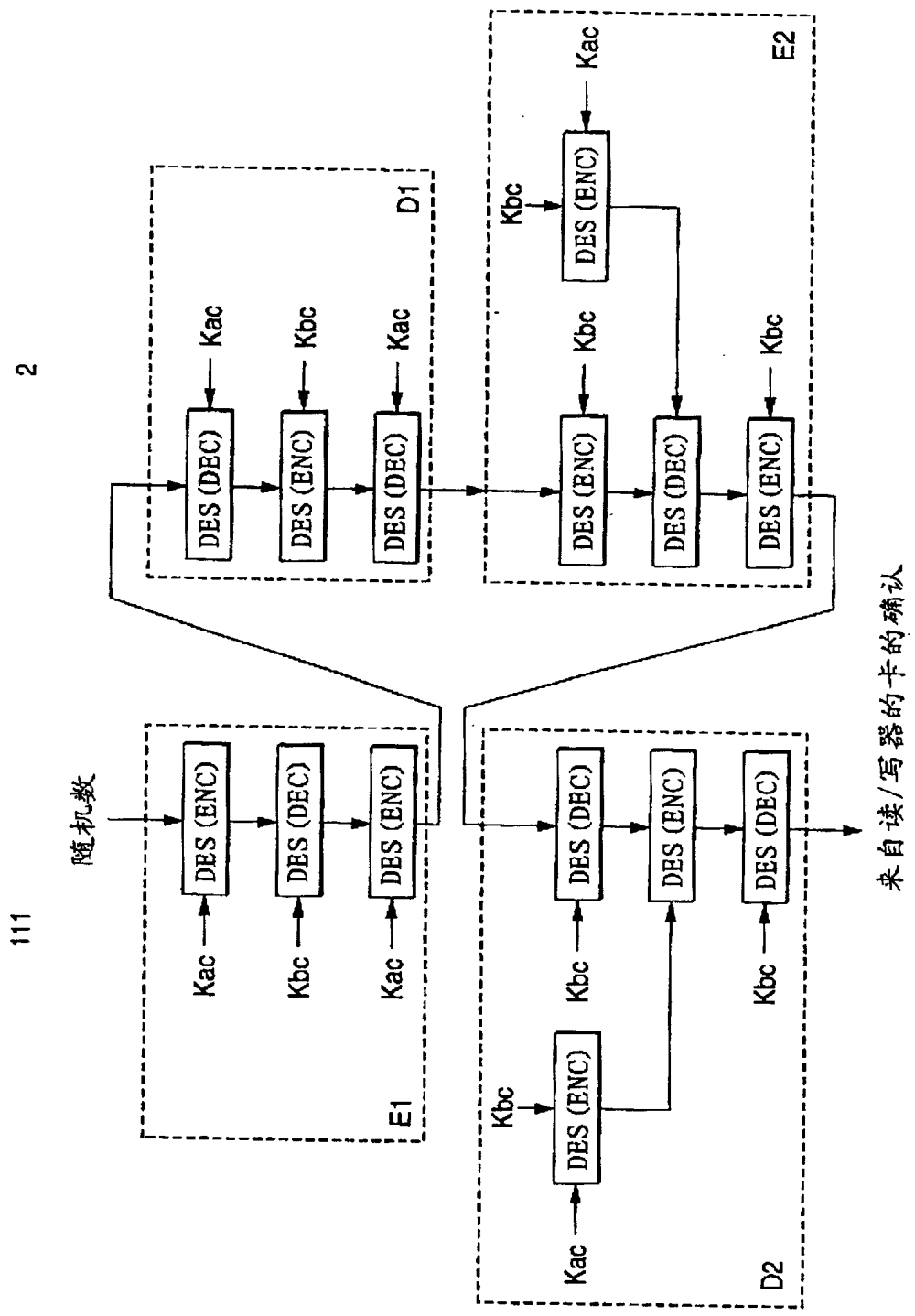


图 14

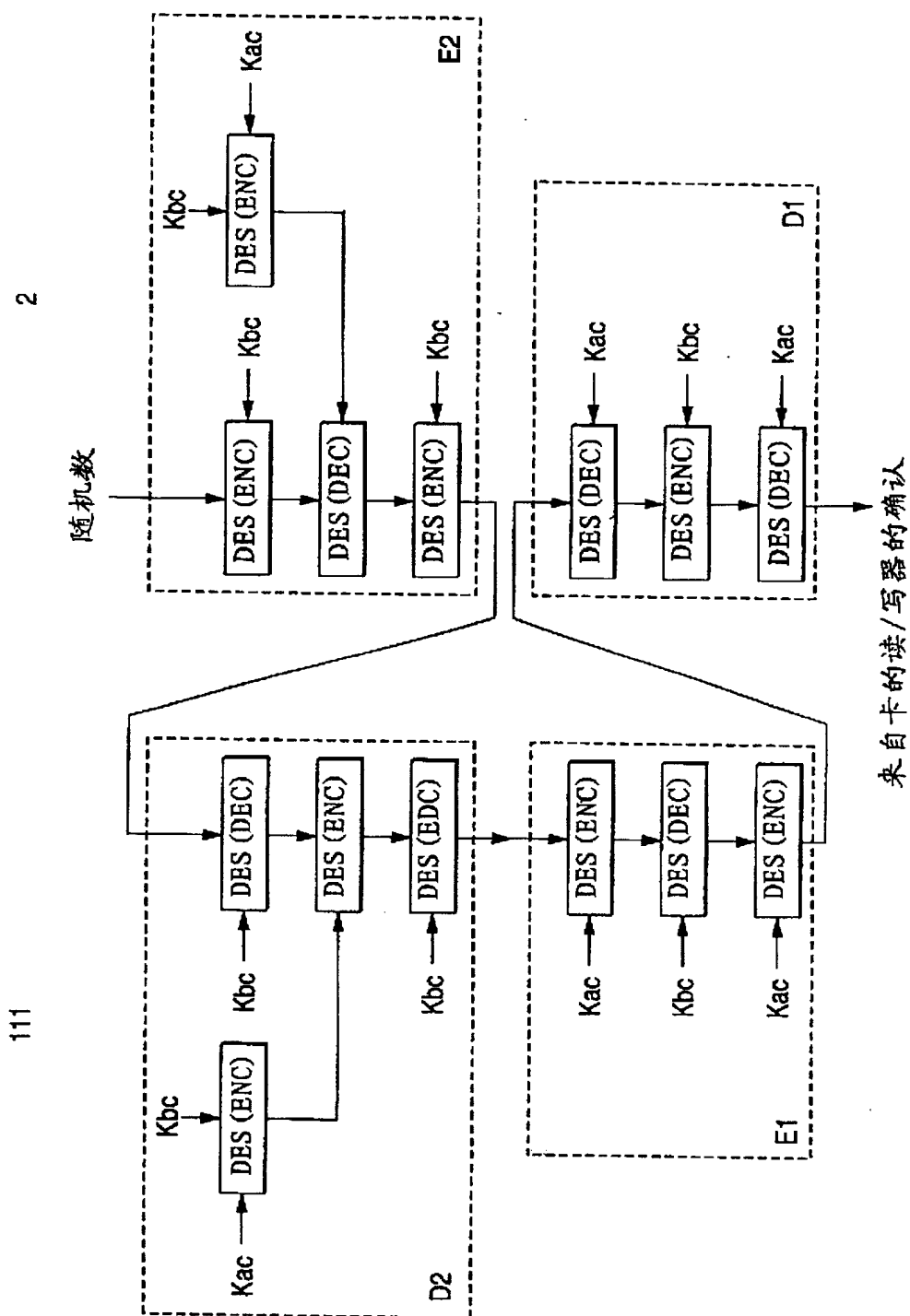


图 15

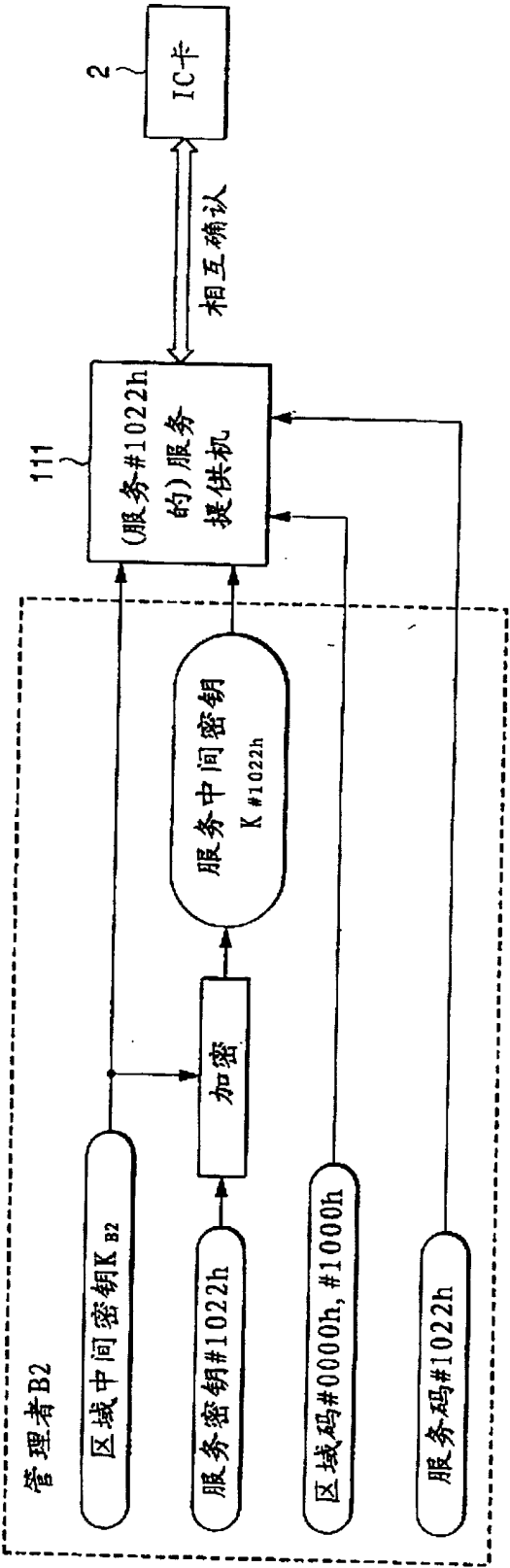


图 16

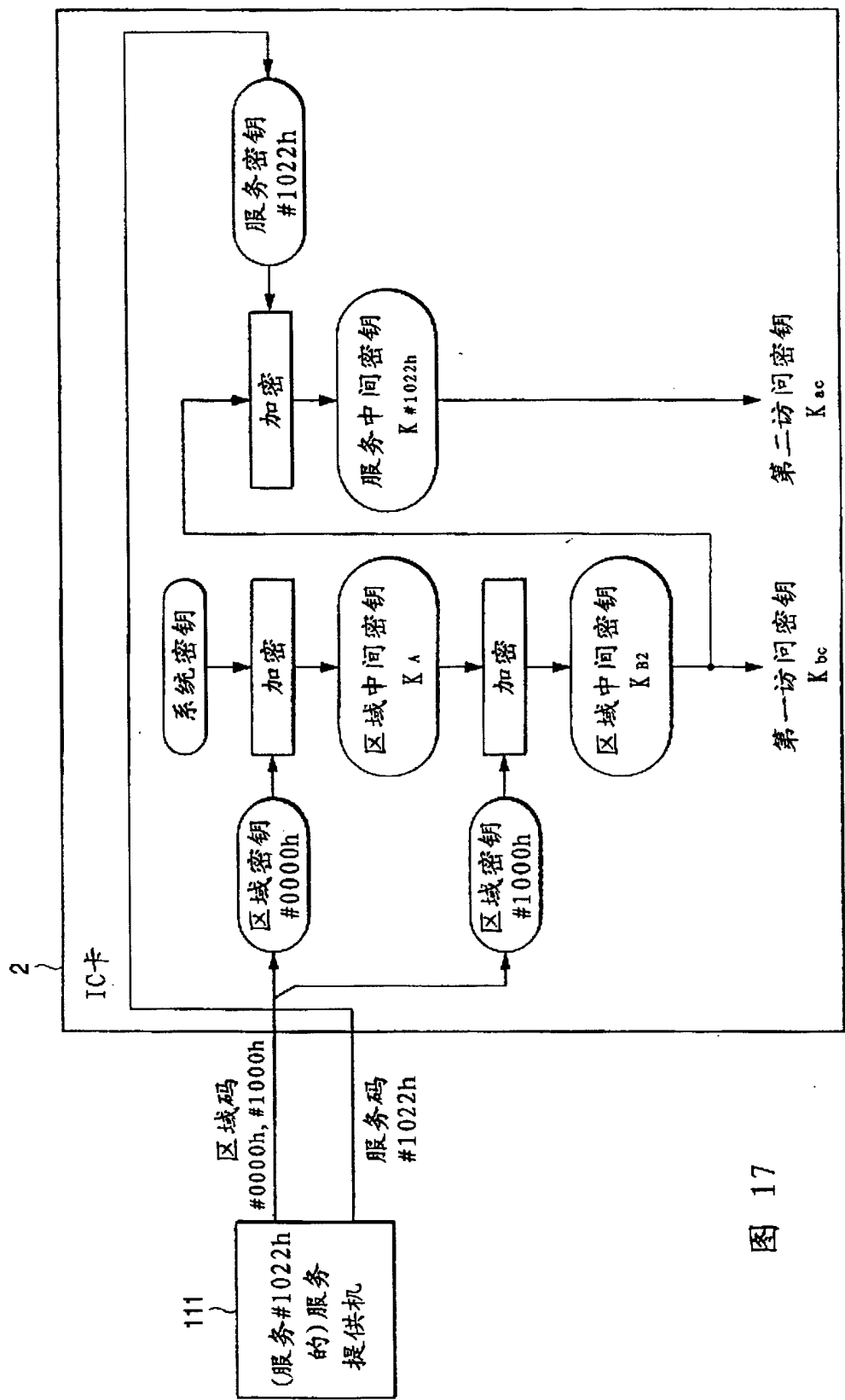


图 17

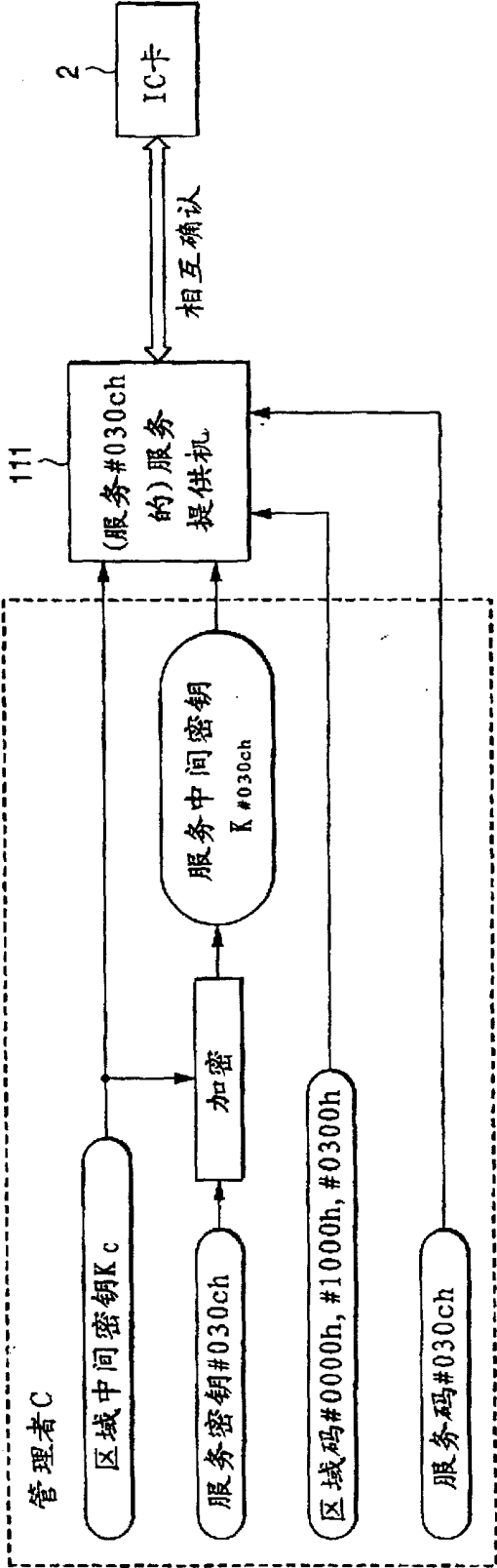


图 18

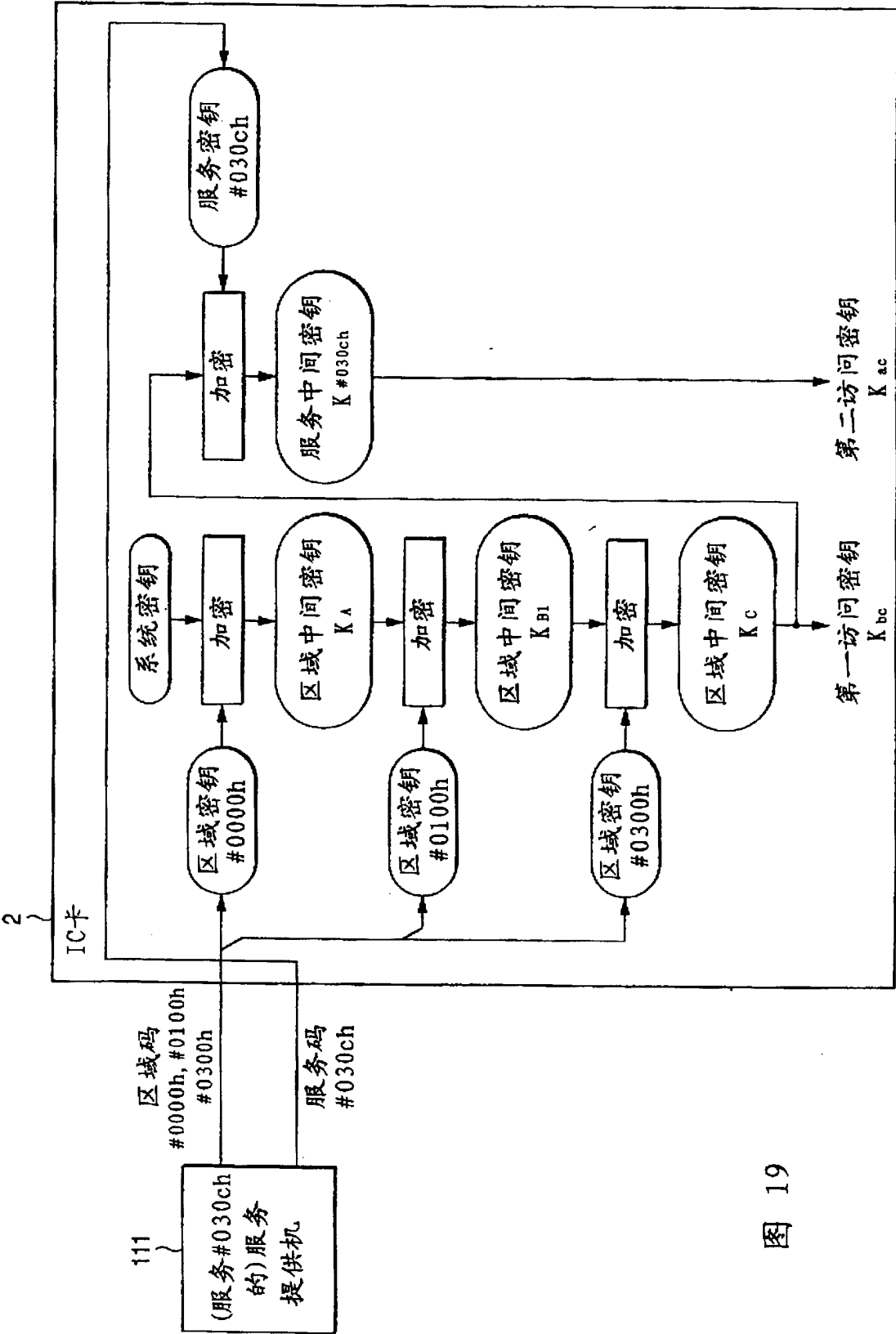


图 19

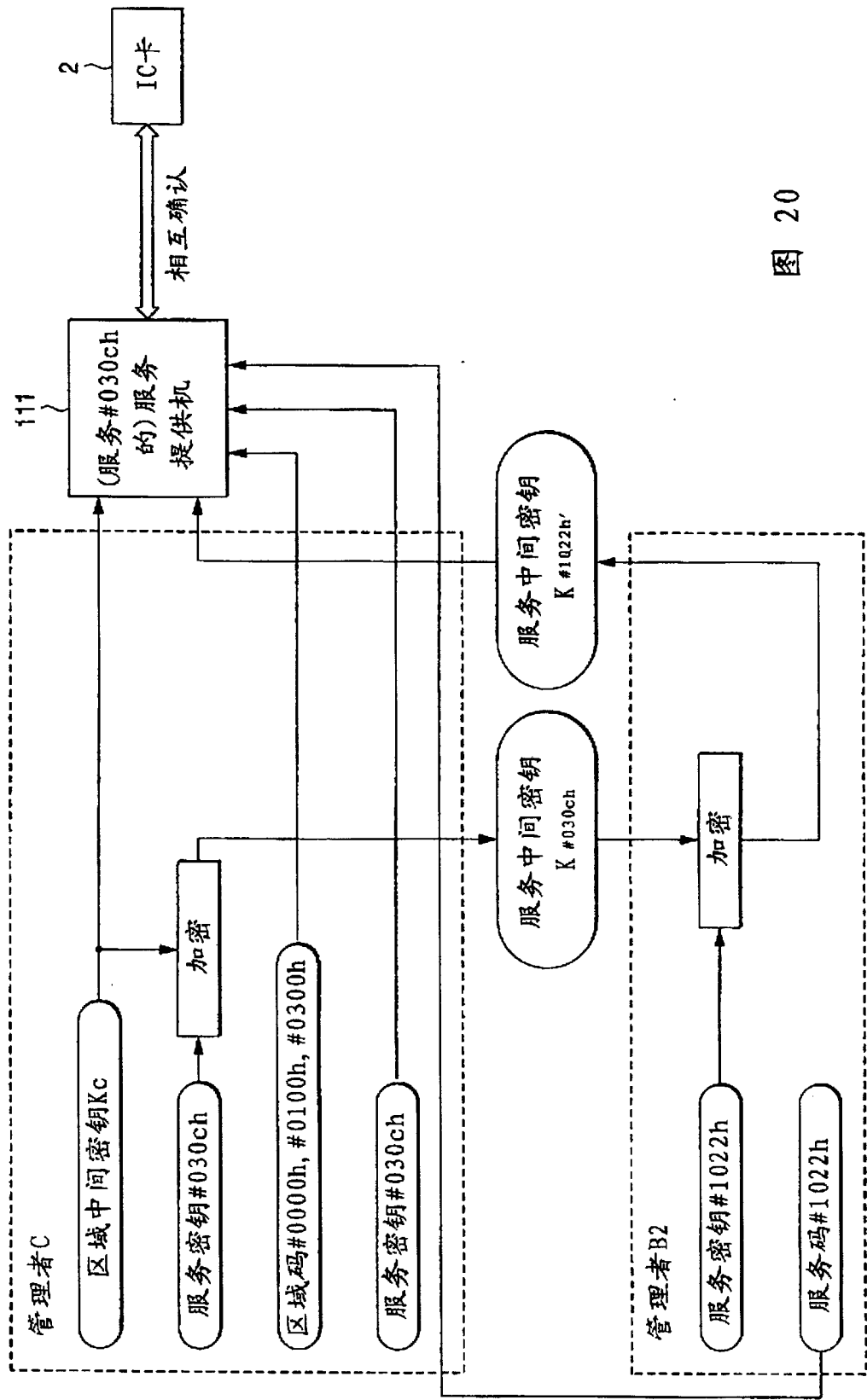


图 20

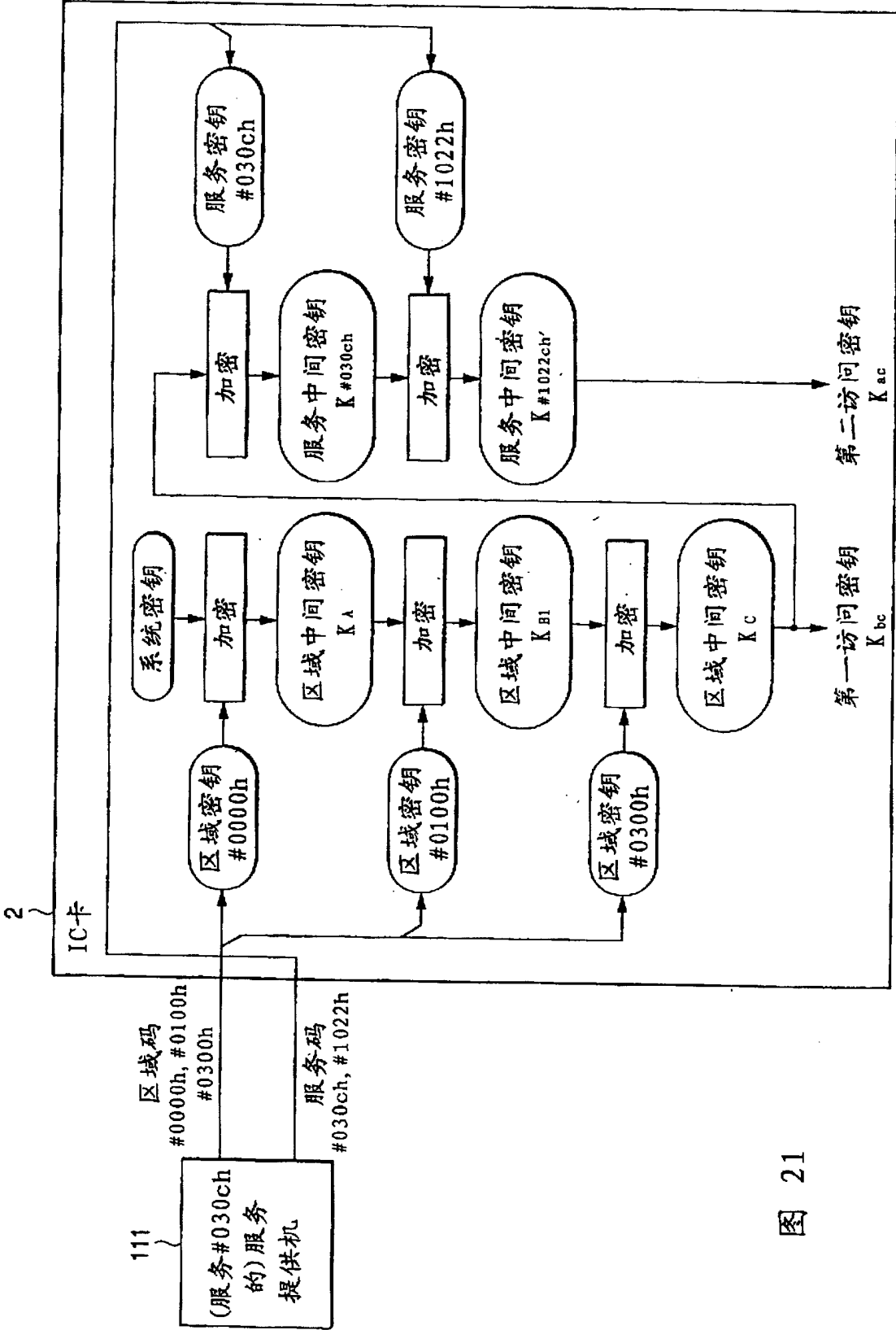


图 21

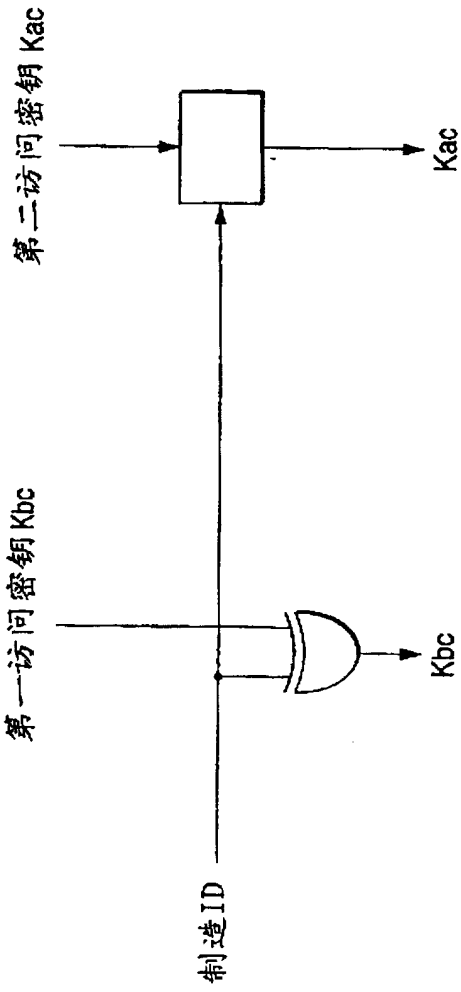


图 22

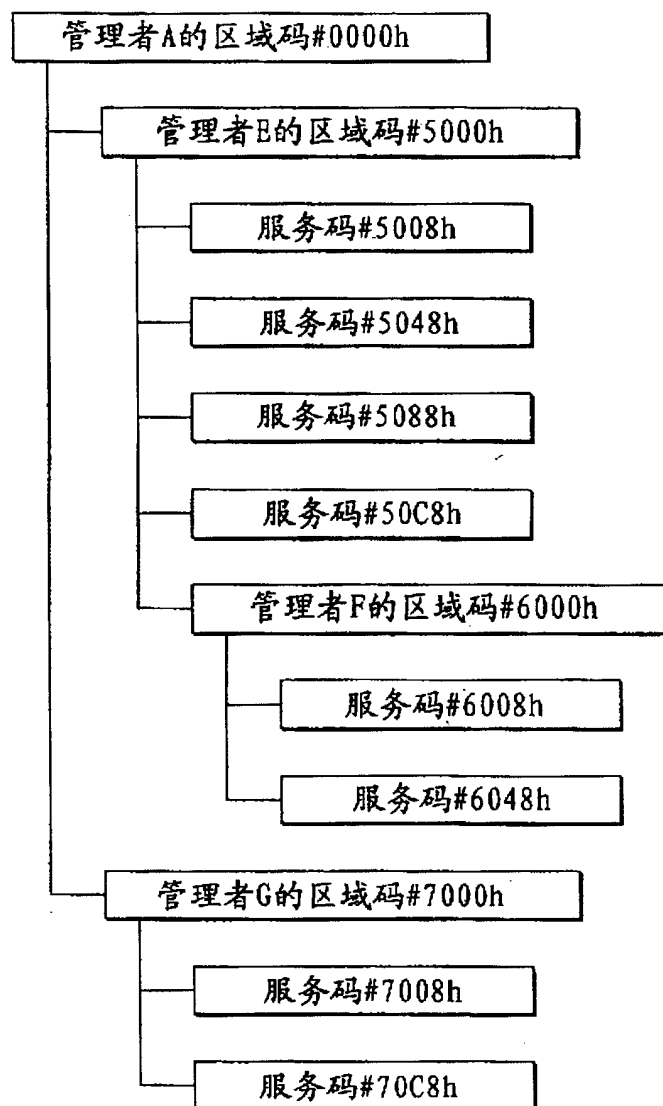
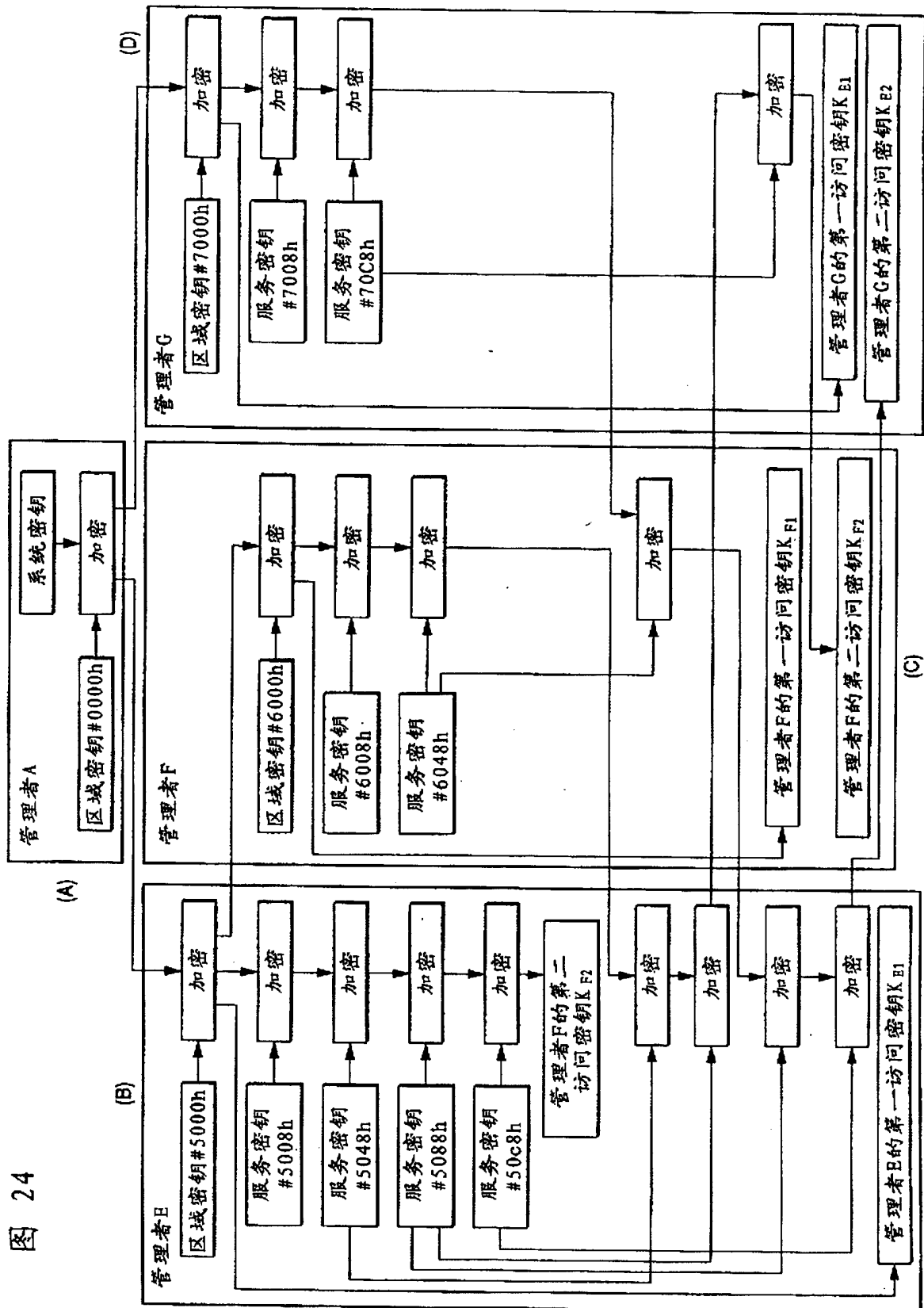


图 23



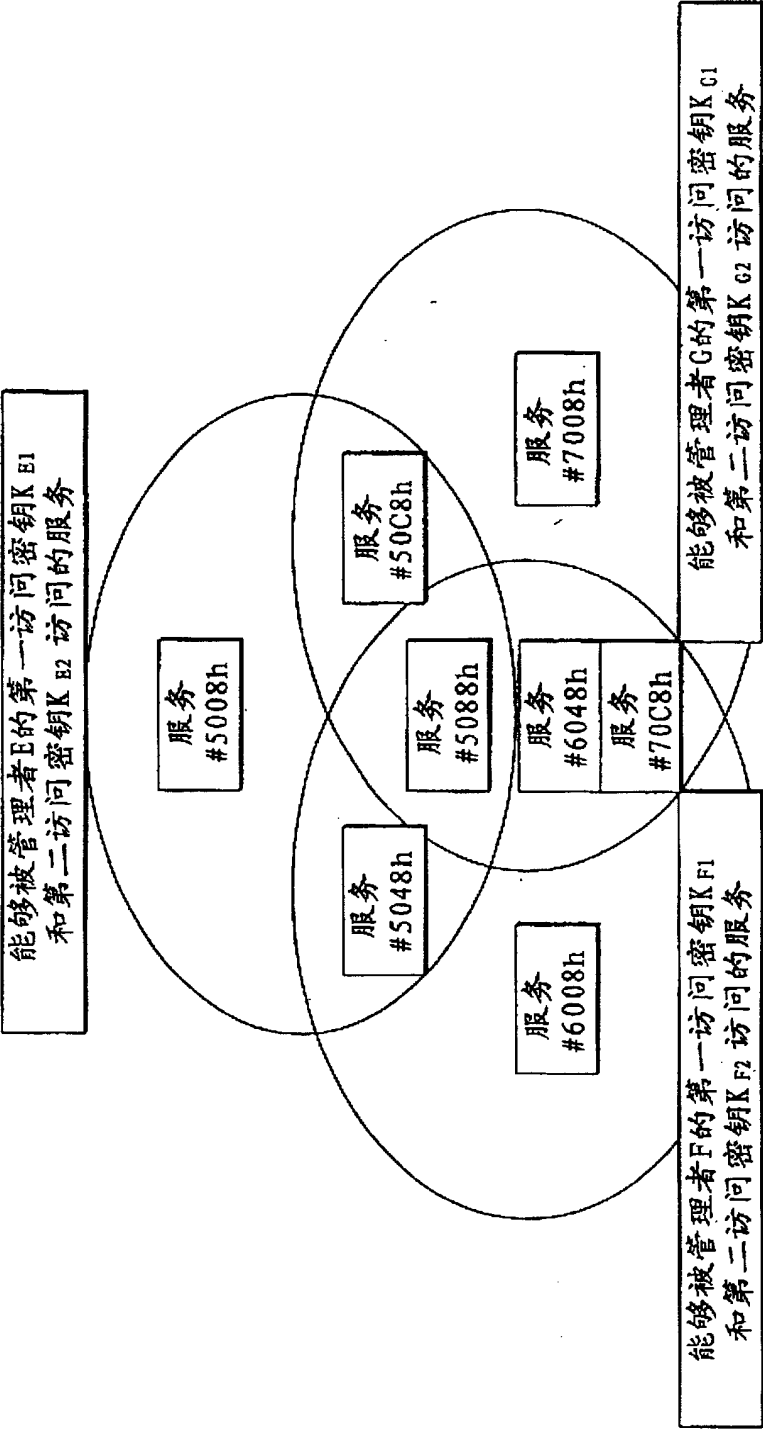


图 25

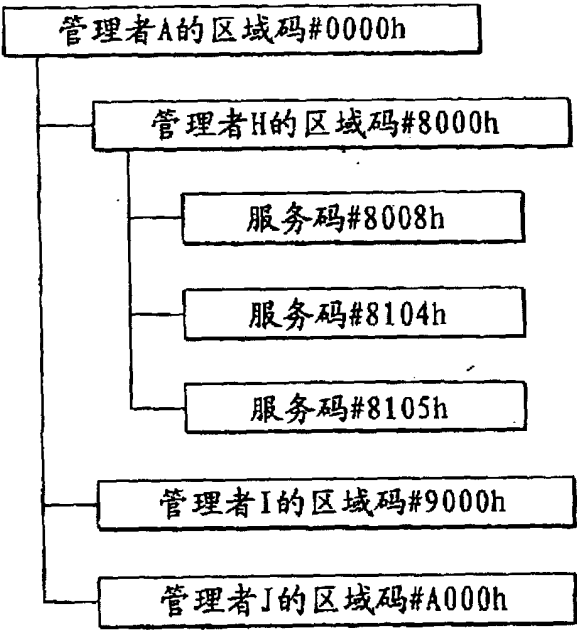


图 26

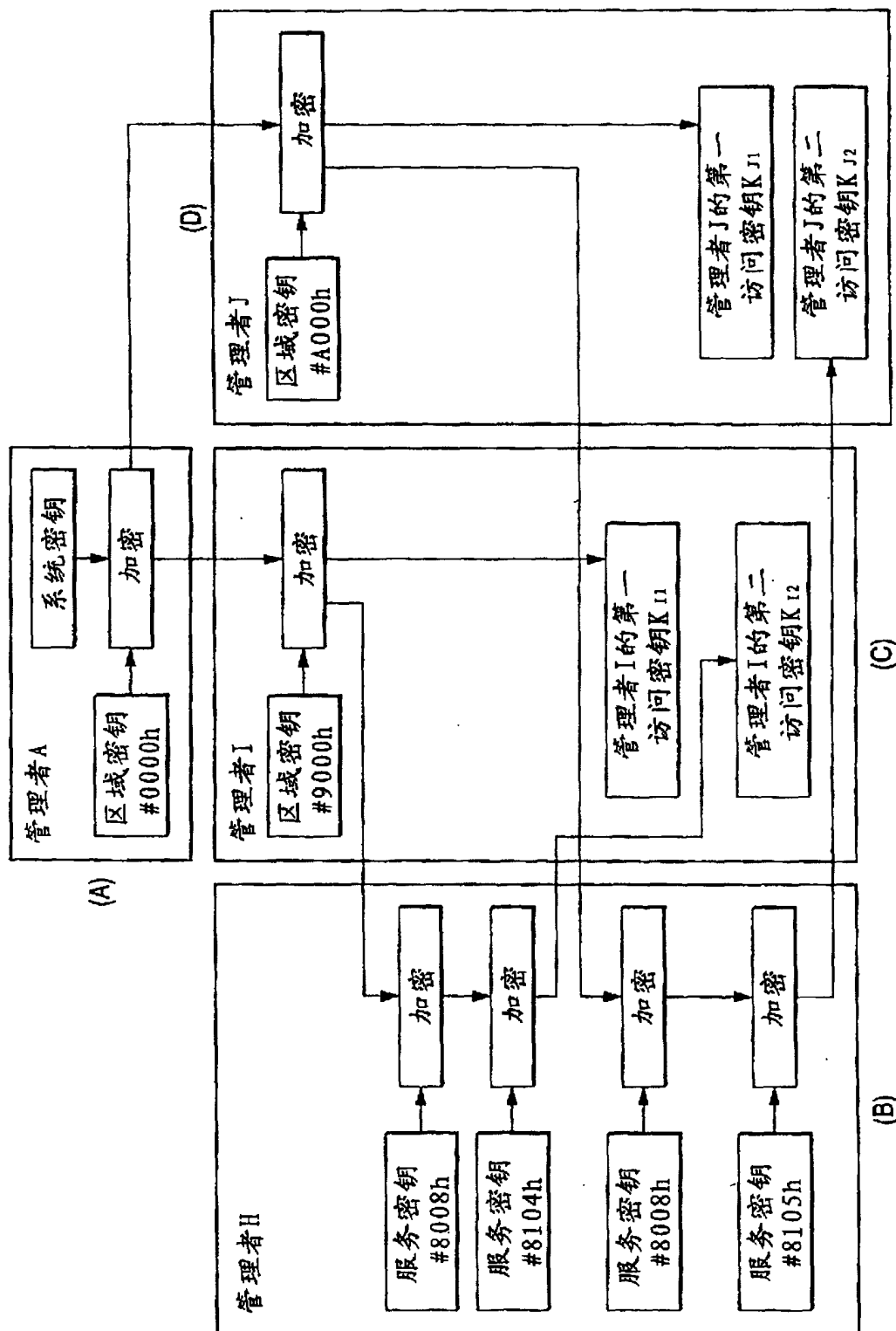


图 27

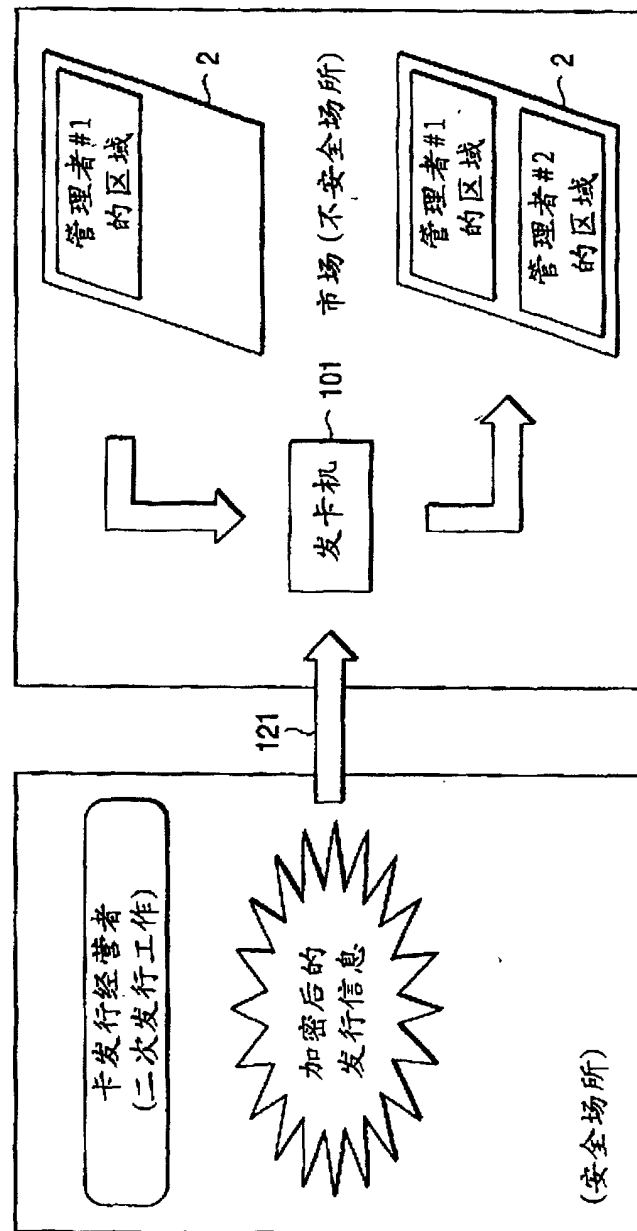


图 28

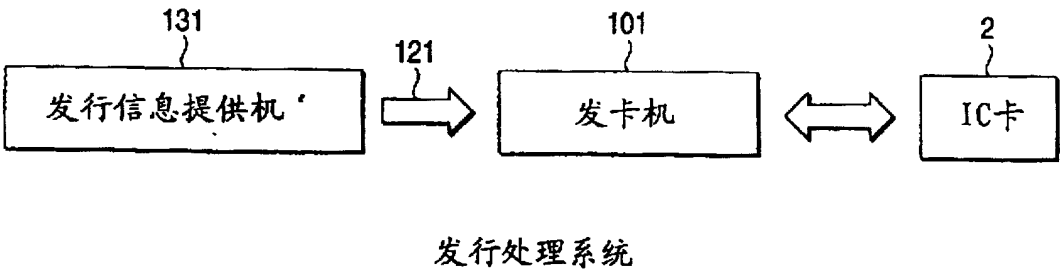


图 29

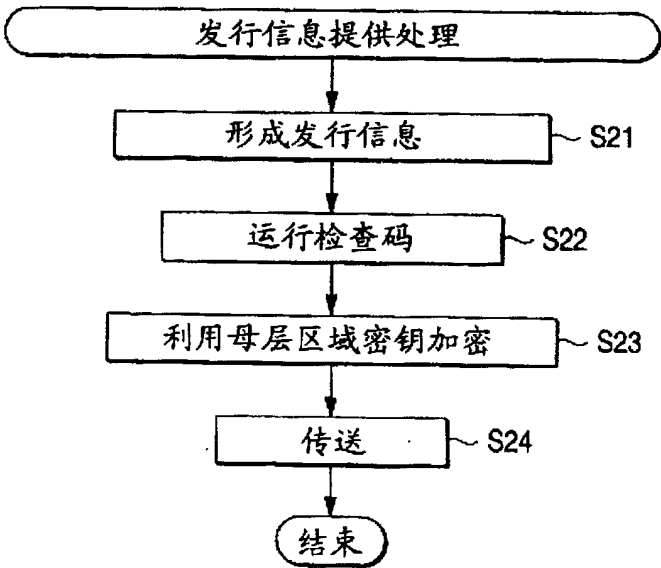
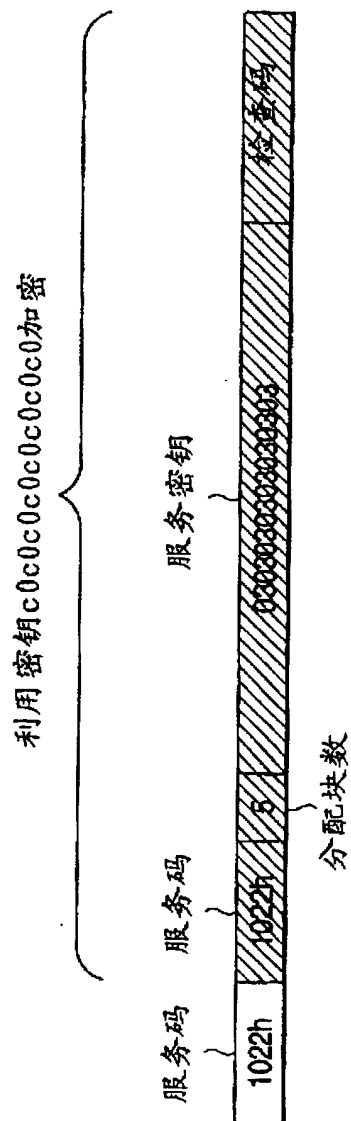
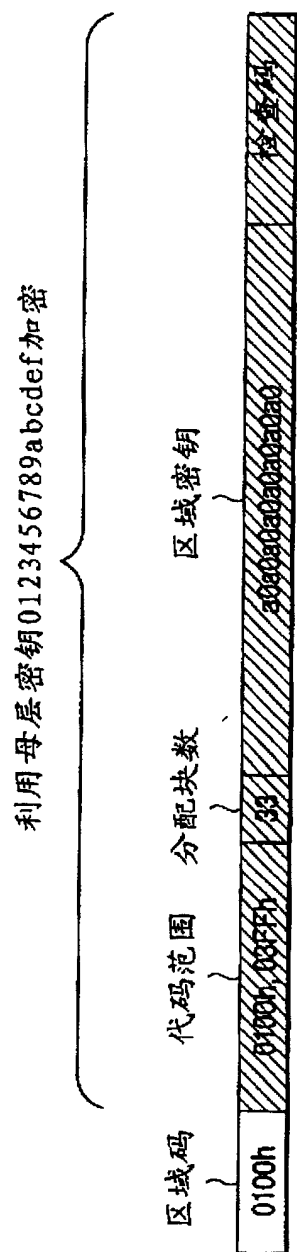


图 30



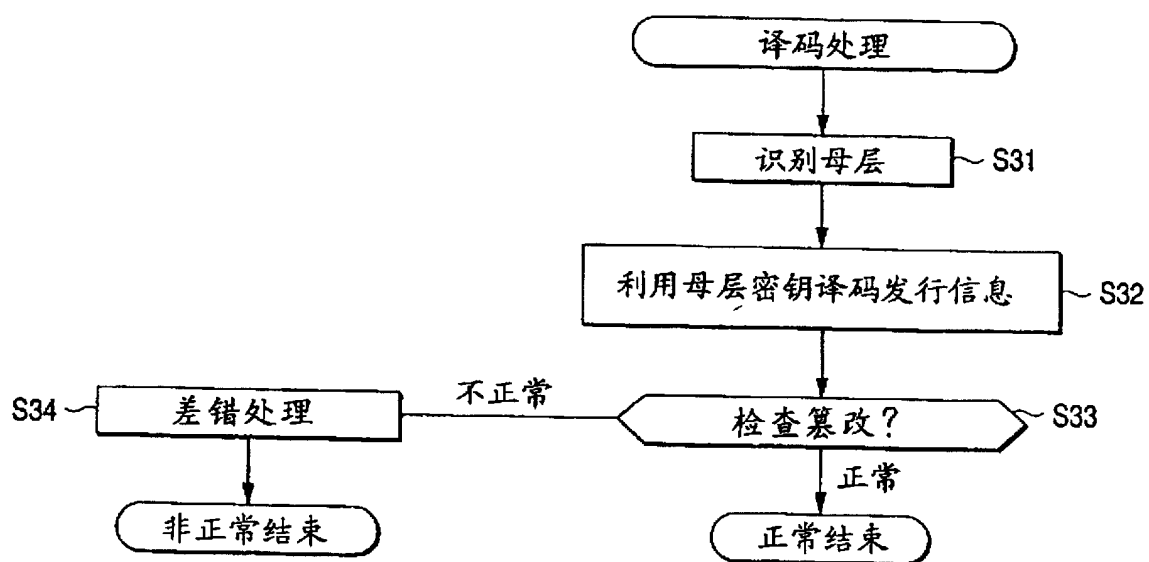


图 32