[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 02820513.8

[43] 公开日 2005 年 1 月 26 日

[11] 公开号 CN 1572099A

[22] 申请日 2002.10.17 [21] 申请号 02820513.8
[30] 优先权
[32] 2001.10.19 [33] JP [31] 321656/2001
[86] 国际申请 PCT/JP2002/010774 2002.10.17
[87] 国际公布 WO2003/036901 英 2003.5.1
[85] 进入国家阶段日期 2004.4.16
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 山本雅哉 三浦康史 中原彻

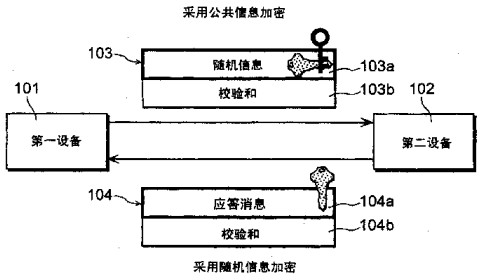
[74] 专利代理机构 永新专利商标代理有限公司
代理人 王 英

权利要求书 11 页 说明书 28 页 附图 13 页

[54] 发明名称 设备鉴别系统和设备鉴别方法

[57] 摘要

从第一设备(101)发送的发射数据(103)包括由公共信息加密的随机信息(103a)以及校验和(103b)，并发送到第二设备(102)。第二设备(102)接收到发射数据(103)，并向第一设备(101)发送回包括采用随机信息(103a)加密的应答消息(104a)和校验和(104b)的应答数据(104)。



ISSN1008-4274

1、一种至少包括第一设备和用于确定第一设备与其是否属于相同组的第二设备的设备鉴别系统，

其中，第一设备包括：

第一公共信息存储单元，用于存储公共信息；

发射数据产生单元，用于产生包括密钥信息的发射数据；

第一加密单元，用于采用公共信息对产生的发射数据进行加密；

第一发射单元，用于将第一加密单元产生的加密发射数据发送给第二设备；

第一解密单元，用于采用密钥信息对从第二设备发送的加密应答数据进行解密；以及，

鉴别单元，用于判断解密的应答数据是否具有一个预定规则，当解密的应答数据具有一个预定规则时，确定第一设备和第二设备属于相同组，以及，

第二设备包括：

第二公共信息存储单元，用于存储公共信息；

第二解密单元，用于采用公共信息对从第一设备发送的加密发射数据进行解密；

判断单元，用于判断解密的发射数据是否具有一个预定规则；

应答数据产生单元，用于当发射数据具有一个预定规则时，确定第一设备和第二设备属于相同组，并产生指示第一设备和第二设备属于相同组的应答数据；

第二加密单元，用于采用在由第二解密单元解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，

第二发射单元，用于将第二加密单元产生的加密的应答数据发送给第一设备。

2、依据权利要求 1 的设备鉴别系统，

其中，发射数据产生单元产生一个随机数，并产生包括产生的作

为密钥信息的随机数的发射数据。

3、依据权利要求 1 的设备鉴别系统，

其中，第一设备进一步包括用于产生发射数据的第一校验和的校验和产生单元，

第一发射单元将第一校验和与加密发射数据一起发送给第二设备，以及，

判断单元通过判断解密的发射数据的第二校验和是否等于从第一设备发送的第一校验和来判断发射数据是否具有预定规则。

4、依据权利要求 1 的设备鉴别系统，

其中，当判断单元判断出解密的发射数据不具有预定规则时，第二设备不向第一设备发送应答数据。

5、依据权利要求 1 的设备鉴别系统，

其中，第一加密单元将发射数据和第一校验和进行合并和加密，

第一发射单元向第二设备发送由第一加密单元产生的加密数据，

第二解密单元采用公共信息将从第一设备发送的加密数据解密成发射数据和第一校验和，以及

判断单元通过判断解密的发射数据的第二校验和是否等于解密的第一校验和来判断发射数据是否具有预定规则。

6、依据权利要求 1 的设备鉴别系统，

其中，发射数据产生单元产生包括预定的固定信息的发射数据，以及

判断单元通过判断包括在解密的发射数据中的固定信息是否具有预定的数据模式来判断发射数据是否具有预定规则。

7、依据权利要求 1 的设备鉴别系统，包括多个第二设备，

其中，第一发射单元向该多个第二设备广播发射数据。

8、依据权利要求 1 的设备鉴别系统，包括多个第二设备，

其中，第一发射单元向该多个第二设备发送发射数据，以及

第一设备进一步包括：

组列表产生单元，用于根据由鉴别单元在该多个第二设备上作出的确定来产生一个指示与第一设备属于相同组的第二设备的列表的组列表；以及

组通信单元，用于根据产生的组列表与第二设备执行预定的通信。

9、依据权利要求 8 的设备鉴别系统，

其中，第一设备进一步控制发射数据产生单元、第一发射单元和组列表产生单元中的至少一个单元，使得在组列表中登记的第二设备的数目不会超过一个预定数目。

10、依据权利要求 1 的设备鉴别系统，

其中，发射数据产生单元使填充数据包括在发射数据中，以便发射数据的尺寸为预定长度，以及

应答数据产生单元使填充数据包括在应答数据中，以便应答数据的尺寸为预定长度。

11、依据权利要求 1 的设备鉴别系统，

其中，发射数据产生单元产生包括指定搜索目标的搜索信息的发射数据，

第二设备进一步包括搜索信息判断单元，用于判断第二设备是否持有包括在解密发射数据中的搜索信息所指示的目标，以及，

应答数据产生单元产生包括由搜索信息判断单元作出的判断的结果的应答数据。

12、依据权利要求 11 的设备鉴别系统，

其中，发射数据产生单元使一个指定数字内容的内容 ID 作为搜

索信息包括在发射数据中，以及，

当第二设备持有许可时，应答数据产生单元使一个指定许可的许可 ID 包括在应答数据中，其中许可是允许利用由包括在发射数据中的内容 ID 所指示的数字内容的权利信息。

13、依据权利要求 12 的设备鉴别系统，

其中，第一设备进一步包括：

许可列表产生单元，用于产生一个指示在从第二设备发送的应答数据中包括的许可 ID 的列表的许可列表；以及

许可发射单元，用于在产生的许可列表的基础上执行与第二设备的用于发送和接收许可的通信。

14、依据权利要求 1 的设备鉴别系统，

其中，第一公共信息存储单元和第二公共信息存储单元中的每一个单元都存储多个不同的公共信息，

第一加密单元采用从存储在第一公共信息存储单元的多个公共信息中选择的一单个公共信息来对发射数据进行加密，以及

第二解密单元采用从存储在第二公共信息存储单元的多个公共信息中选择的一单个公共信息来对发射数据进行解密。

15 依据权利要求 14 的设备鉴别系统，

其中，发射数据产生单元产生包括指定数字内容的搜索信息和该内容使用形式的发射数据，

第二设备进一步包括搜索信息判断单元，用于判断第二设备是否持有由解密的发射数据中包括的搜索信息所指示的许可，其中许可是允许以所述使用形式利用数字内容的权利信息，

应答数据产生单元产生包括由搜索信息判断单元作出的判断的结果的应答数据，

第一加密单元从存储在第一公共信息存储单元的多个公共信息中选择对应于使用形式的一单个公共信息，并采用所选择的公共信息

对发射数据加密，以及

第二解密单元从存储在第二公共信息存储单元的多个公共信息中选择对应于使用形式的一单个公共信息，并采用所选择的公共信息对发射数据解密。

16、依据权利要求 15 的设备鉴别系统，

其中，第一设备进一步包括第一公共信息编辑单元，用于执行对存储在第一公共信息存储单元中的公共信息的添加和删除，以及

第二设备进一步包括第二公共信息编辑单元，用于执行对存储在第二公共信息存储单元中的公共信息的添加和删除。

17、一种用于一个至少包括第一设备和用于确定第一设备与其是否属于相同组的第二设备的系统的设备鉴别方法，

其中，第一设备和第二设备中的每一个分别包括存储公共信息的第一公共信息存储单元和第二公共信息存储单元，

该设备鉴别方法包括由第一设备执行的第一步骤和由第二设备执行的第二步骤，以及

第一步骤包括：

发射数据产生步骤，用于产生包括密钥信息的发射数据；

第一加密步骤，用于采用公共信息对产生的发射数据进行加密；

第一发射步骤，用于将第一加密步骤产生的加密的发射数据发送给第二设备；

第一解密步骤，用于采用密钥信息对从第二设备发送的加密的应答数据进行解密；以及，

鉴别步骤，用于判断解密的应答数据是否具有一个预定规则，当解密的应答数据具有一个预定规则时，确定第一设备和第二设备属于相同组，以及，

第二步骤包括：

第二解密步骤，用于采用公共信息对从第一设备发送的加密的发射数据进行解密；

判断步骤，用于判断解密的发射数据是否具有一个预定规则；

应答数据产生步骤，用于当发射数据具有一个预定规则时，确定第一设备和第二设备属于相同组，并产生指示第一设备和第二设备属于相同组的应答数据；

第二加密步骤，用于采用在由解密步骤解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，

第二发射步骤，用于将第二加密步骤产生的加密的应答数据发送给第一设备。

18、依据权利要求 17 的设备鉴别方法，

其中，在发射数据产生步骤中，产生一个随机数，并产生包括产生的作为密钥信息的随机数的发射数据。

19、依据权利要求 17 的设备鉴别方法，进一步包括一个校验和产生步骤，用于在第一设备中产生发射数据的第一校验和，

其中，在第一发射步骤中，将第一校验和与加密发射数据一起发送给第二设备，以及，

在判断步骤中，通过判断解密的发射数据的第二校验和是否等于从第一设备发送的第一校验和来判断解密的发射数据是否具有预定规则。

20、依据权利要求 17 的设备鉴别方法，

其中，在第一加密步骤中，将发射数据和第一校验和进行合并和加密，

在第一发射步骤中，向第二设备发送在第一加密步骤中产生的加密数据，

在第二解密步骤中，采用公共信息将从第一设备发送的加密数据解密成发射数据和第一校验和，以及

在判断步骤中，通过判断解密的发射数据的第二校验和是否等于解密的第一校验和来判断解密的发射数据是否具有预定规则。

21、依据权利要求 17 的设备鉴别方法，

其中，系统包括多个第二设备，

在第一发射步骤中，向该多个第二设备发送发射数据，以及

第一步骤进一步包括：

组列表产生步骤，用于根据在鉴别步骤中在该多个第二设备上作出的确定来产生一个指示与第一设备属于相同组的第二设备的列表的组列表；以及

组通信步骤，用于根据产生的组列表与第二设备执行预定的通信。

22、依据权利要求 17 的设备鉴别方法，

其中，在发射数据产生步骤中，产生包括指定搜索目标的搜索信息的发射数据，

在该设备鉴别方法中，第二步骤进一步包括搜索信息判断步骤，用于判断第二设备是否持有由解密发射数据中包括的搜索信息所指示的目标，以及，

在应答数据产生步骤中，产生包括在搜索信息判断步骤作出的判断的结果的应答数据。

23、依据权利要求 22 的设备鉴别方法，

其中，在发射数据产生步骤中，将一个指定数字内容的内容 ID 作为搜索信息包括在发射数据中，以及，

在应答数据产生步骤中，当第二设备持有许可时，将一个指定许可的许可 ID 包括在应答数据中，其中许可是允许利用由在发射数据中包括的内容 ID 所指示的数字内容的权利信息。

24、依据权利要求 17 的设备鉴别方法，

其中，第一公共信息存储单元和第二公共信息存储单元中的每一个单元都存储多个不同的公共信息，

在第一加密步骤中，采用从存储在第一公共信息存储单元的多个公共信息中选择的一单个公共信息来对发射数据进行加密，以及

在第二解密步骤中，采用从存储在第二公共信息存储单元的多个公共信息中选择的一单个公共信息来对发射数据进行解密。

25、一种用于通过与伙伴设备相互鉴别来确定伙伴设备与其自身是否属于相同组的通信设备，包括：

鉴别单元，用于鉴别伙伴设备；以及

鉴别目标单元，用于由伙伴设备鉴别，以及

其中，鉴别单元包括：

公共信息存储单元，用于存储公共信息；

发射数据产生单元，用于产生包括密钥信息的发射数据；

第一加密单元，用于采用公共信息对产生的发射数据进行加密；

第一发射单元，用于将第一加密单元产生的加密的发射数据发送给伙伴设备；

第一解密单元，用于采用密钥信息对从伙伴设备发送的加密的应答数据进行解密；以及，

鉴别单元，用于判断解密的应答数据是否具有一个预定规则，当解密的应答数据具有一个预定规则时，确定伙伴设备与该设备自身属于相同组，以及，

鉴别目标单元包括：

第二解密单元，用于采用公共信息对从伙伴设备发送的加密的发射数据进行解密；

判断单元，用于判断解密的发射数据是否具有一个预定规则；

应答数据产生单元，用于当发射数据具有一个预定规则时，确定伙伴设备与该设备自身属于相同组，并产生指示伙伴设备与该设备自身属于相同组的应答数据；

第二加密单元，用于采用在由解密单元解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，

第二发射单元，用于将第二加密单元产生的加密的应答数据发送

给伙伴设备。

26、依据权利要求25的通信设备，

其中，发射数据产生单元产生一个随机数，并产生包括产生的作为密钥信息的随机数的发射数据。

27、依据权利要求25的通信设备，

其中，伙伴设备进一步包括用于产生发射数据的第一校验和的校验和产生单元，

第一发射单元将第一校验和与加密的发射数据一起发送给伙伴设备，以及，

判断单元通过判断解密的发射数据的第二校验和是否等于从伙伴设备发送的第一校验和来判断解密的发射数据是否具有预定规则。

28、一种用于通信设备通过与伙伴设备相互鉴别来确定伙伴设备和该设备自身是否属于相同组的程序，该程序包括：

鉴别步骤，用于鉴别伙伴设备；以及

鉴别目标步骤，用于由伙伴设备鉴别，以及

其中，鉴别步骤包括：

发射数据产生步骤，用于产生包括密钥信息的发射数据；

第一加密步骤，用于采用事先存储的公共信息对产生的发射数据进行加密；

第一发射步骤，用于将在第一加密步骤产生的加密的发射数据发送给伙伴设备；

第一解密步骤，用于采用密钥信息对从伙伴设备发送的加密的应答数据进行解密；以及，

鉴别步骤，用于判断解密的应答数据是否具有一个预定规则，当解密的应答数据具有一个预定规则时，确定伙伴设备与该设备自身属于相同组，以及，

鉴别目标步骤包括：

第二解密步骤，用于采用公共信息对从伙伴设备发送的加密的发射数据进行解密；

判断步骤，用于判断解密的发射数据是否具有一个预定规则；

应答数据产生步骤，用于当发射数据具有一个预定规则时，确定伙伴设备与该设备自身属于相同组，并产生指示伙伴设备与该设备自身属于相同组的应答数据；

第二加密步骤，用于采用在解密步骤中解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，

第二发射步骤，用于将在第二加密步骤产生的加密的应答数据发送给伙伴设备。

29、依据权利要求 28 的程序，

其中，发射数据产生步骤产生一个随机数，并产生包括产生的作为密钥信息的随机数的发射数据。

30、依据权利要求 28 的程序，进一步包括用于产生发射数据的第一校验和的校验和产生步骤，

其中，在第一发射步骤中，将第一校验和与加密的发射数据一起发送给伙伴设备，以及，

在判断步骤中，通过判断解密的发射数据的第二校验和是否等于从伙伴设备发送的第一校验和来判断解密的发射数据是否具有预定规则。

31.一种计算机可读记录介质，用于至少包括第一设备和用于确定第一设备与其是否属于相同组的第二设备的设备鉴别系统，

其中，鉴别数据记录在该计算机可读记录介质中，包括：

包括密钥信息并采用公共信息进行加密的加密发射数据；以及

发射数据的校验和，

鉴别数据是从第一设备向第二设备发送的数据，

当第二设备确定第一设备与第二设备属于相同组时，密钥信息用

于对从第二设备向第一设备发送的应答数据进行加密，以及

公共信息是由属于相同组的设备事先持有的信息。

32、依据权利要求 31 的记录介质，

其中，密钥信息是由第一设备产生的随机数。

33、依据权利要求 31 的记录介质，

其中，发射数据包括一个指定数字内容的内容 ID，以及，

应答数据包括一个指定许可的许可 ID，其中许可是允许利用由在发射数据中包括的内容 ID 所指示的数字内容的权利信息。

设备鉴别系统和设备鉴别方法

技术领域

本发明涉及一种在每个设备鉴别相同网络内的其他设备时所需的设备鉴别系统，本发明尤其涉及一种在多个终端之间使用的设备鉴别系统。

背景技术

近年来，诸如音乐、电影和游戏的数字内容可以通过经由因特网、数字广播或分组媒体的分发来容易地获得。当在多个终端之间复制或移动这些数字内容及其权利时，通常不允许无限制地移动它们，而是允许仅仅在一特定范围内复制或移动。

通常认为，复制和移动只有在由一单个用户所拥有的多个终端之间是被允许的。为了实现这种只在一特定范围内允许复制和移动的限制，需要形成一组终端，其中在这个组内相互之间的复制和移动是被允许的。

迄今，已经假设这种类型的组确定由一个服务器（组确定终端）来执行。下面简要解释一下由服务器执行的组确定处理。

常规的组确定系统包括一个确定组的服务器以及由服务器控制并与其相连以便可以通过网络进行通信的多个终端。服务器保存属于每个组的终端的组列表。组列表的意思例如是将一个组标识符与终端标识符相联系的信息。

在如上所构造的组确定系统中，组确定的实现如下。首先，为了使一个受控终端获得该终端自身所属的设备的组列表，该终端向服务器发送一个终端列表请求数据。在这个终端列表请求数据中，包括诸如终端自己的终端标识符和组标识符之类的信息。根据在终端列表请

求数据中包括的信息，服务器向请求的终端发送一个对应于该信息的组列表。通过这些过程获得它所属的组的组信息之后，受控终端能够实现组确定。

例如，在常规的用于识别组的成员标识方法中，主机终端广播包括所有成员的名字以及主机终端所特有的网络地址的分组数据。然后，每个成员终端分析所接收的分组并识别从一个具有其名字的分组中检索出的信息，并将一个包括每个成员的名字和每个成员终端所特有的网络地址的分组作为数据发送给主机终端。然后，主机终端分析所接收的分组，如果它发现属于相同组的成员的名字，则获得在该分组中包括的信息，将成员名字与一个终端地址相对应，并保存相应的数据（例如，参见日本公开的专利申请 No. H10-23028 作为参考）。

首先，解释一下这个常规的组确定方法所具有的问题，即，在这个方法中，在服务器终端（组确定终端）与受该服务器控制的终端之间存在着父子关系，因此服务器终端与受控终端必须具有不同的功能。

其次，考虑将常规的确定方法运用到通常由最终用户使用的家用电器上的情况。为了运用常规的确定方法，用户必须理解他/她所拥有的家用电器的父子关系，并且在他/她购买任何家用电器时必须考虑如何在电器之间设置父子关系。这是因为在组确定中服务器终端是不可缺少的，并且假定服务器终端和受控终端在功能和价格上是不同的。

基本上，对于诸如家用电器之类的时常增加的并且可以假定具有各种用途的终端，终端之间的关系应该是平等的。然而，当所有终端都是平等关系时，没有已知的用于创建一个组的常规方法。

现在，考虑上述问题，当终端彼此具有平等关系时，依据本发明的设备鉴别系统使得终端能够确定属于相同组的其他终端。

并且，在依据本发明的设备鉴别系统中，其目的是一个终端在它进行诸如鉴别或内容传送的给终端带来繁重负担的处理之前能够以安全方式获得属于相同组的设备的列表。此外，在依据本发明的设备鉴别系统中，其目的是通过采用上述的组列表，一个终端能够确定它

将把发射数据发送给哪个设备，并通过不与不被允许获得特定内容的终端进行通信来实现通信信道的有效利用。

本发明的目的还在于提供一个能够对收费内容的网络分发的未来普及有贡献的设备鉴别系统。

发明公开

为了实现上述目的，本发明是至少包括第一设备以及用于确定第一设备与其是否属于相同组的第二设备的设备鉴别系统，其中，第一设备包括：第一公共信息存储单元，用于存储公共信息；发射数据产生单元，用于产生包括密钥信息的发射数据；第一加密单元，用于使用公共信息对产生的发射数据进行加密；第一发射单元，用于将第一加密单元产生的加密发射数据发送给第二设备；第一解密单元，用于采用密钥信息对从第二设备发送的加密应答数据进行解密；以及，鉴别单元，用于判断解密的应答数据是否具有一个预定规则，当解密的应答数据具有一个预定规则时，确定第一设备和第二设备属于相同组，以及，第二设备包括：第二公共信息存储单元，用于存储公共信息；第二解密单元，用于使用公共信息对从第一设备发送的加密的发射数据进行解密；判断单元，用于判断解密的发射数据是否具有一个预定规则；应答数据产生单元，用于当发射数据具有一个预定规则时，确定第一设备和第二设备属于相同组，并产生指示第一设备和第二设备属于相同组的应答数据；第二加密单元，用于采用在由第二解密单元解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，第二发射单元，用于将第二加密单元产生的加密的应答数据发送给第一设备。

而且，为了实现上述目的，本发明是设备鉴别系统，其中，发射数据产生单元产生一个随机数，并产生包括产生的作为密钥信息的随机数的发射数据。此外，本发明是设备鉴别系统，其中，第一设备进一步包括用于产生发射数据的第一校验和的校验和产生单元，第一发射单元将第一校验和以及加密的发射数据发送给第二设备，以及，判

断单元通过判断解密的发射数据的第二校验和是否等于从第一设备发送的第一校验和来判断发射数据是否具有预定规则。

另外，为了实现上述目的，本发明是包括多个第二设备的设备鉴别系统，其中，第一发射单元向该多个第二设备广播发射数据。

此外，为了实现上述目的，本发明是设备鉴别系统，其中，发射数据产生单元产生包括指定搜索目标的搜索信息的发射数据，第二设备进一步包括搜索信息判断单元，用于判断第二设备是否保存有在解密的发射数据中包括的搜索信息所指示的目标，以及，应答数据产生单元产生包括由搜索信息判断单元作出的判断的结果的应答数据。

同样，为了实现上述目的，本发明是设备鉴别系统，其中，发射数据产生单元使一个指定数字内容的内容 ID 作为搜索信息包括在发射数据中，以及，当第二设备持有许可时，应答数据产生单元使一个指定许可的许可 ID 包括在应答数据中，其中许可是允许利用在发射数据中包括的内容 ID 所指示的数字内容的权利信息。

此外，本发明不仅可以实现为上述设备鉴别系统，还可以实现为具有在设备鉴别系统中所包括的步骤的设备鉴别方法，以及在一个设备上实现所述单元的通信设备。

不必说，本发明也可以被实现为一个在计算机等上实现设备鉴别方法的程序，或者可以通过诸如 CD-ROM 的记录介质或诸如通信网络的传输介质来分发该程序。

附图简要说明

从下面的结合图示本发明的具体实施例的附图的描述，本发明的这些和其他目的、优点和特征将变得明显。在附图中：

图 1 是解释依据第一实施例的设备鉴别系统的示例图。

图 2 是显示依据第一实施例的多个设备和组的关系的示意图。

图 3 是显示依据第一实施例的第一设备的详细结构的方框图。

图 4 是显示依据第一实施例的第二设备的详细结构的方框图。

图 5 是显示依据第一实施例的发射数据的数据结构的示意图。

图 6 是显示依据第一实施例的应答数据的数据结构的示意图。

图 7A 是显示依据第一实施例的用户接口的屏幕的示意图。

图 7B 是显示依据第一实施例的用户接口的另一个屏幕的示意图。

图 8A 是显示依据第一实施例的由第一设备创建的组列表的信息项目的示意图。

图 8B 是显示依据第一实施例的由第一设备创建的另一个组列表的信息项目的示意图。

图 9 是显示依据第一实施例的设备鉴别系统的组确定处理的流程图。

图 10 是显示依据第二实施例的第三设备的详细结构的方框图。

图 11 是显示依据第二实施例的第四设备的详细结构的方框图。

图 12 是显示依据第二实施例的发射数据的数据结构的示意图。

图 13 是显示依据第二实施例的应答数据的数据结构的示意图。

图 14 是显示依据第二实施例的当第三设备采用搜索信息向第四设备和第五设备进行许可搜索时进行的发射过程的序列图。

图 15 是显示依据第二实施例的设备鉴别系统的组确定处理的流程图。

实现发明的最佳方式

下面参考用于理解本发明的附图来解释用于实现本发明的最佳方式。然而，下面的实施例只是实现本发明的一些例子，而不是限制本发明的技术领域。下面参考附图解释实现本发明的最佳方式。

在详细解释之前，先定义本发明中的“组”。如果有在彼此之间允许诸如复制或移动内容或内容的权利的处理的终端，则在逻辑上有可能将这些终端“编组”。将这些“编组”的终端的单位称为“授权域”，为简单起见，下面将其称为“组”。

（第一实施例）

图 1 是解释依据本发明的第一实施例的设备鉴别系统的示例图。在图 1 中，将第一设备 101 和第二设备 102 连接，使得可以通过有线或无线的传输信道进行数据传输。这里，第一设备 101 代表确定其他终端是否与它自己属于相同组的设备，第二设备 102 代表对作为查询设备查询它是否属于相同组的设备作出响应的设备。虽然在这个第一实施例中，采用两个终端，第一设备 101 和第二设备 102 进行解释，但对于在广播可达到的区域内的所有终端都可以通过同样的方法进行设备鉴别。

第一设备 101 例如可以是由最终用户使用的设备，例如 PC、移动电话或机顶盒。这个第一设备 101 是实现编组并创建组列表的设备。为了实现编组，它创建发射数据 103，对发射数据 103 加密，并将其发送给第二设备 102。

第二设备 102 与第一设备 101 类似，是一个在广播可达到的区域内的诸如 PC、移动电话或机顶盒之类的终端。它接收从第一设备 101 发送的发射数据 103，创建并加密应答数据 104，并将数据发送回第一设备 101。

发射数据 103 包括随机信息 103a 和校验和 103b。这个随机信息 103a 由诸如口令之类的第一设备 101 产生的随机字节串的公共信息进行加密。校验和 103b 是将诸如随机信息 103a 的数据分块并将每块中的数据变换成数值并相加然后发送出去的信息。在这个第一实施例中，校验和 103b 在发送之前不加密，但也可以在发送之前用公共信息等对校验和 103b 加密。

应答数据 104 是对从第一设备 101 发送的信息作出响应的数据，它包括应答消息 104a 和校验和 104b。在应答消息 104a 中，包括诸如关于证明设备在相同组内的信息，并采用已经接收到的随机信息 103a 对其加密。校验和 104b 与校验和 103b 类似，是在发送之前将诸如应答消息 104a 的数据分块并将每块中的数据变换成数值并相加的信息。在本实施例中，该信息在发回之前不加密。

下面利用图 2 解释第一设备 101 如何确定其他设备是否与它自身属于相同组的流程。在第一实施例中，一个设备是否属于相同组的差

别取决于该设备是否持有公共信息 A。这意味着，为了采用本发明的方法实现组确定处理，假设属于相同组的所有设备都持有公共信息 A。

图 2 是显示依据第一实施例的多个设备和组的关系的示意图。这里，在这个设备鉴别系统中，有第一设备 101、第二设备 102、第六设备 201 和第七设备 202。在第一实施例中，第一设备 101 代表一个实现对与它自身属于相同组的其他设备的过滤的设备，并且它通过广播确定其他设备是否与它自身属于相同组。在图 2 中，第一设备 101 和第二设备 102 属于相同组，授权域 1，而第七设备 202 属于另一组，授权域 2。

第一设备 101 是一个诸如 PC 的终端，它向第二设备 102 和第七设备 202 广播采用公共信息 A 加密的发射数据，它们俩都在广播可达到的区域内并允许数据传输。这里，允许传输的范围例如包括在每个家庭内使用的家庭网络。

第二设备 102 持有公共信息 A，能够对已经采用这个公共信息 A 加密的发射数据进行解密。不考虑任何传输错误，第二设备 102 能够向第一设备 101 发送回正确的应答数据。当第一设备 101 接收到应答数据时，它通过实现某些规定处理来确定第二设备 102 与它自身属于相同组。

由于第七设备 202 持有不同于公共信息 A 的公共信息 C，所以当它接收到已经采用公共信息 A 加密的发射数据时，在第七设备 202 的校验和确定单元实现的规定处理的结果将是“不相等”，因而不发送回任何应答数据。即使当在第七设备 202 实现的校验和确定的结果由于巧合而“相同”时，在第一设备 101 实现的校验和确定也是“不相等的”，因此第七设备 202 将不会作为属于相同组的设备添加到列表中。同时，在广播可达到的区域之外的第六设备 201 将不会被确定为在相同组中，因为发射数据不会到达该设备。

采用上述的确定方法，第一设备 101 能够创建与它自身属于相同组的设备的列表，而不必发送公共信息 A。可以保证在组列表中包括的所有设备至少持有公共信息 A，因而保证它们都属于相同组。

下面将分别解释第一设备 101 和第二设备 102 的详细结构。

图 3 是显示依据第一实施例的第一设备的详细结构的方框图。第一设备 101 是一个实现广播并创建与它自身属于相同组的设备的列表的终端。第一设备 101 包括产生随机字节串的随机信息产生单元 301、加密/解密单元 302、存储诸如口令的公共信息的公共信息存储单元 303、校验和产生单元 304、设备间通信单元 305 以及校验和确定单元 306。校验和是在发送之前将数据分块并将每块中的数据变换成数值然后相加的信息。

首先，解释当第一设备 101 向第二设备 102 发送出发射数据 T-Data 1 时的数据流。

随机信息产生单元 301 创建随机字节串，并将它们用作随机信息 R1，例如会话密钥信息和填充数据。这个随机信息 R1 保存在这个单元中直到暂停时间（time-out）结束。这里，暂停时间指的是从产生随机信息 R1 开始该设备将等待来自其他设备的响应的等待时间，其由用户或设备制造商设置。同时，随机信息产生单元 301 向校验和产生单元 304 和加密/解密单元 302 发送随机信息 R1。

加密/解密单元 302 采用公共信息 A 对随机信息 R1 加密，并将这个加密的信息 E1 发送给设备间通信单元 305。公共信息存储单元 303 具有硬盘等来存储公共信息 A。这个公共信息 A 通常由服务器端保存，而不是由用户输入，该信息将在用户签约或购买一个设备时由服务器端输入到公共信息存储单元 303。

校验和产生单元 304 通过对所接收的随机信息 R1 的每块校验和目标部分内的数据求和来产生 CS1，并将这个 CS1 发送给设备间通信单元 305。设备间通信单元 305 然后根据接收的校验和 CS1 和加密信息 E1 制作成发射数据 T-Data 1 的一个分组，并将其作为发射数据 T-Data 1 发送到第二设备 102。

接着，解释当第一设备 101 接收到已经从第二设备 102 发回的应答数据 A-Data 2 时的数据流。

首先，设备间通信单元 305 在另一个设备，即第二设备 102 之间进行数据传输。当它从第二设备 102 接收应答数据 A-Data 2 时，设

备间通信单元305向加密/解密单元302发送加密的信息E2以供解密，并将应答数据 A-Data 2 所附带的 CS3 发送给校验和确定单元 306。

加密/解密单元 302 采用随机信息 R1 对加密信息 E2 解密，并将解密的应答数据 DA2 发送给校验和产生单元 304。然后，校验和产生单元 304 通过对所接收的解密的应答数据 DA2 的每块校验和目标部分内的数据的数值求和来产生 CS4，并将这个 CS4 发送给校验和确定单元 306。

校验和确定单元 306 保存一个组列表，一个存储属于相同组的设备的存储单元。它比较上述的 CS3 和 CS4，如果两个校验和值相等，则它将第二设备 102 作为属于相同组的设备添加到组列表中。在两个校验和的值不相等的情况下，它确定第二设备 102 不属于与它自身相同的组，因而不将其添加到组列表中。

在前面的句子中，提到解密的应答数据DA2由加密/解密单元302发送。然而，校验和确定单元 306 可以发送获取请求。

图 4 是显示依据第一实施例的第二设备 102 的详细结构的方框图。除了与第一设备 101 类似的加密/解密单元 402、公共信息存储单元 403、校验和产生单元 404、设备间通信单元 405 和校验和确定单元 406 之外，第二设备 102 还包括应答数据产生单元 407，其产生包括诸如关于证实它属于相同组的信息的应答数据 AD。这里，在第二设备 102 中不包括在第一设备 101 中包括的随机信息产生单元 301。

下面解释已经由第二设备102从第一设备101接收到的发射数据 T-Data 1 的流程。当设备间通信单元 405 接收到发射数据 T-Data 1 时，它将发射数据 T-Data 1 中的加密信息 E1 发送给加密/解密单元 402，将发射数据 T-Data 1 中的 CS1 发送给校验和确定单元 406。

加密/解密单元 402 采用存储在公共信息存储单元 403 中的公共信息 A 对加密信息 E1 解密，并将解密数据 DR1 发送给校验和产生单元 404。

校验和产生单元 404 然后通过对解密数据 DR1 的每块校验和目标部分内的数据的数值求和来产生 CS2，并将这个 CS2 发送给校验和确定单元 406。校验和确定单元 406 将前述的 CS1 与 CS2 进行比

较，如果相等，校验和确定单元 406 指示应答数据产生单元 407 创建应答数据 AD，因为发射数据 T-Data 1 现在被确认为是从属于相同组的设备发送的数据。

沿着这个方向，应答数据产生单元 407 产生包括诸如关于证实它属于相同组的数据的应答数据 AD，并将这个应答数据 AD 发送到加密/解密单元 402 和校验和产生单元 404。加密/解密单元 402 采用在加密信息 E1 中包括的随机信息 R1 对应答数据 AD 加密，并将其作为加密数据 E2 发送给设备间通信单元 405。同时，校验和产生单元 404 通过对应答数据 AD 的每块校验和目标部分内的数据的数值求和来产生 CS3，并将其发送给设备间通信单元 405。替代采用随机信息 R1，也可以采用公共信息 A 来实现加密。

设备间通信单元 405 然后产生一个包括加密数据 E2 和 CS3 的应答数据 A-Data 2 的分组，并将其发送回第一设备 101。这是在设备鉴别系统中实现的一系列数据处理的结束。

图 5 是显示依据第一实施例的发射数据 T-Data 1 的数据结构的示意图。注意，这个图被作为例子呈现以解释第一实施例。

发射数据 T-Data 1 是一个从第一设备 101 向其他设备发送的、要求其他设备就它们是否属于与第一设备 101 相同的组作出响应的消息。它包括消息首部 501、客户 ID 502、随机信息 503、填充数据 504 和校验和 505。

消息首部 501 包括诸如查询接收设备是否属于相同组的消息。它位于发射数据 T-Data 1 的头部，被不加密地发送。客户 ID 502 保存第一设备 101，即消息的发送者的客户 ID。

随机信息 503 由随机字节串组成，它包括诸如在对应答数据加密时采用的会话密钥的信息。这个会话密钥信息在第一设备 101 中维持直到暂停时间（time-out）结束为止，并且用于对应答数据的加密部分进行解密。

填充数据 504 是备用数据。例如，其加密算法是 AES，当发射数据 T-Data 1 的数据长度不是 8 字节，即加密单位的倍数时，将其附在后面，使得发射数据 T-Data 1 变为 8 字节的倍数。它由公共信息加密，

为了提高加密强度，加密目标数据部分 ED 可以采用填充数据 504 延长。也可以设置一个大约 2 字节的保留字段来代替对填充数据 504 的使用。

校验和 505 保存在包括客户 ID 502、随机信息 503 和填充数据 504 的每块校验和目标部分 CT 内的数据的数值的和。并且，可以采用诸如 SHA-1 或 MD 5 的散列函数来代替诸如 CRC32 的校验和算法。

加密目标数据 ED 包括客户 ID 502、随机信息 503 和填充数据 504，至少包括随机信息 503。并且，在这个加密目标数据 ED 中，还可以包括唯一地识别网络上的第一设备 101 的设备标识信息。具体地，这个设备标识信息可以是它自己的 IP 地址或客户 ID 502、设备的标识符等。如果需要 IP 地址，例如，当发送回应答数据时，则也可以在发射数据 T-Data 1 中包括 IP 地址。

下面采用图 6 解释应答数据 A-Data 2 的内容。图 6 是显示依据第一实施例的应答数据 A-Data 2 的数据结构的示意图。注意，这个图仅作为例子进行呈现以解释该实施例，本发明并不限于这个结构。

应答数据 A-Data 2 是对发射数据 T-Data 1、即从第一设备 101 发送的应答请求消息的答复。应答数据 A-Data 2 包括消息首部 601、客户 ID 602、公共信息 603、填充数据 604 和校验和 605。

消息首部 601 包括诸如关于接收设备是否属于相同组的消息的信息，客户 ID 602 是第二设备 102、应答数据 A-Data 2 的发送者的客户 ID。公共信息 603 是由第一设备 101 和第二设备 102 共同持有的诸如口令的公共信息，在这个第一实施例中，它是公共信息 A。

填充数据 604 是备用数据，为了提高加密强度，应答数据 AD 可以采用填充数据 604 延长。校验和 505 是在包括客户 ID 602、随机信息 603 和填充数据 604 的每块校验和目标部分 CT 内的数据的数值的和。

应答数据 AD 包括客户 ID 602、公共信息 603 和填充数据 604，包括公共信息 603 是为了确认第二设备 102 持有公共信息 A。在发送回之前采用在前述的随机信息 503 中包括的会话密钥等对这个应答数据 AD 加密。

并且，应答数据 AD 至少包括用于唯一地识别网络上的第二设备 102 的设备标识信息。这里，设备标识信息例如可以是它自己的 IP 地址或客户 ID 602，即设备的标识符。然而，虽然在前面的句子中提到应答数据 AD 至少包括设备标识信息，但这是不需要的，如果当多个设备通信时符合给定的通信协议的消息首部包括等效于设备标识信息的信息（例如，它自己的 IP 地址）。

下面，作为对使用本发明的设备鉴别系统的准备，这里给出如何对设备设置公共信息的一些例子。

图 7A 和 7B 是显示在这个第一实施例中的用户接口的屏幕的示例图。在这种情况下，假设组的设置范围是通常由相同个用户拥有的多个设备。为了实现组设置，用户想方设法获得公共信息并将信息通过图 7A 所示的 UI 输入到属于相同组的设备。为了限制对设备实现公共信息设置的用户，还可以设置口令等。例如如图 7B 中所示，由用户获得公共信息的方法可以是显示设备的公共信息（在这种情况下，是“zeppetstore”）并将该信息输入到将属于相同组的其他设备中。用户还可以通过邮政、电子邮件等从设备制造商或销售商代销店获得公共信息，或者用户可以创建他们自己的公共信息，并将该信息设置给属于相同组的设备。

另一种可能性是，不将公共信息给用户，而是当设备被发货或销售时根据用户的请求或制造商或销售商代销店的政策由设备制造商或销售商代销店设置。公共信息也可以存储在 IC 卡中，可以通过从插入的 IC 卡读入信息来在每个设备上进行设置。如同已经在前面的关于获得公共信息的句子中所提到的，假设可以用各种可能的途径来获得 IC 卡。还可以使用诸如压缩闪存的存储介质或允许安全数据管理的其他存储介质来代替对 IC 卡的使用。

然而，通常假定公共信息不是由用户输入，而是由服务器端进行管理，并且在用户加入组或购买 PC 的时候通过传输通道自动输入给每个终端。如果用户知道公共信息，则存在着用户将故意增大属于相同组的设备的数目的可能性，因此这种方法将防止这种情况发生。

下面解释关于由第一设备 101 创建的组列表的信息表项的内容

的一个例子。

图 8A 和 8B 是显示在这个实施例中由第一设备 101 创建的组列表的信息表项的示例图。在图 8A 中，有一个标识该组的组 ID 的表项（801a），这个组 ID（801a）描述了属于该组的设备的标识信息。至于设备的标识信息，则描述了诸如设备 ID（802a，803a）的信息。并且，对应于组 ID（801a），可以描述在该组内允许的处理。在图 8A 的情况下，这个允许的处理是“复制”，其他可能的处理包括“再现”或“移动”。

类似地，在图 8B 中，有一个标识该组的组 ID 的表项（811b），对于这个组 ID（811b），将诸如设备 ID（812b，813b）的信息描述为属于该组的设备的标识信息。在图 8B 中，在组内允许的处理是“移动”。

每个设备也可以属于多个组，在这种情况下，每个设备保存对应于多个组的多个公共信息，并且通过规定的处理，每个设备持有多个组列表是可能的。

一旦完成组列表，就在列表中包括的设备之间实现通信并执行在组内等允许的处理。在安全的条件下将采用公用的方法实现诸如鉴别或内容获取的后续处理。如果在每次进行包括复制或移动的任何处理时产生一个组列表并在处理完成之后立即删除，则有可能在每次进行任何处理时获得最新的组信息。

在这个第一实施例中，对用于组设置和组确定的方法的解释是面向用户的，但也可能的是，从内容持有者的视点看，不希望扩大组的区域。在这种情况下，可以设置能够在组列表中描述的设备标识信息的最大值，并且可以使得，每次在基于来自其他终端的应答数据创建一个组列表时，当它达到最大值时强制结束组列表的产生处理。当这些处理是在设备总是正确地运行并且网络结构也是不变的前提下进行的时，用户能够将属于相同组的设备的数目设置为仅仅到最大值加上少数几个。至少，这使得能够防止一组内的设备数无限制地增大。

上面已经解释了对于相同组的设置，但基本上能够通过新输入或删除公共信息来非常灵活和容易地设置属于相同组的设备。

下面解释其结构如上所述的依据第一实施例的设备鉴别系统的操作。

图 9 是显示依据第一实施例的设备鉴别系统的组确定的过程的流程图。在这个第一实施例中，虽然基于第一设备 101 确定第二设备 102 是否属于相同组进行说明，但通过采用类似的设备鉴别系统，也可以经由广播等实现多个终端之间的组确定。并且，在解释设备鉴别系统的操作时，参考在图 3 和 4 中所使用的代码。

首先，包括在第一设备 101 中的随机信息产生单元 301 产生随机信息 R1，并将该信息发送到也包括在第一设备 101 中的加密/解密单元 302 和校验和产生单元 304（S901）。在这个第一实施例中，随机信息产生单元 301 必须维护随机信息 R1 直到暂停时间（time-out）结束。或者，甚至在暂停时间（time-out）结束之前，可以根据用户给出的结束指示，从随机信息产生单元 301 删除随机信息 R1。随机信息 R1 是几个字节的随机字节串，字节数取决于用于加密/解密处理的加密算法等。

当加密/解密单元 302 从随机信息产生单元 301 接收到随机信息 R1 时，它向公共信息存储单元 303 发出公共信息获得请求，然后从公共信息存储单元 303 接收公共信息 A。接着，加密/解密单元 302 通过采用公共信息 A 作为密钥对至少包括随机信息 R1 的加密目标数据 ED 加密来产生加密信息 E1，并将加密数据发送到设备间通信单元 305（S902）。这里，对于加密算法，通常采用对于实际使用具有足够的加密强度的算法，其中的例子有 DES、三重 DES 和 AES。在下面的解释中，虽然假设加密/解密单元 302 和图 4 中的加密/解密单元 402 持有一个相同的加密算法，但它们也可以持有多个加密算法。然而，在持有多个加密算法的情况下，需要加密算法标识符，并且第一设备 101 和第二设备 102 都必须持有对应于上述加密算法标识符的相同的加密算法。

接着，校验和产生单元 304 产生上述至少包括随机信息 R1 的加密目标数据 ED 的 CS1，并将其发送给设备间通信单元 305（S903）。

当设备间通信单元 305 接收到加密信息 E1 和 CS1 时，它向其他

设备发送至少包括加密信息E1和CS1并具有附带的符合通信协议的消息首部等的发射数据T-Data 1（S904）。

现在，当包括在第二设备102中的设备间通信单元405从第一设备101接收到发射数据T-Data 1时，它从发射数据T-Data 1提取出加密信息E1和CS1（S905）。

然后，设备间通信单元405将加密信息E1发送到加密/解密单元402，将CS1发送到校验和确定单元406，这两个单元都包括在第二设备102中。

当加密/解密单元402接收到加密信息E1时，它向公共信息存储单元403发送公共信息获得请求，并从公共信息存储单元403接收公共信息A。加密/解密单元402然后采用公共信息A作为密钥对加密信息E1解密，并获得解密的加密信息（下面称为“解密的加密目标数据”）DR1，将其发送到校验和产生单元404（S906）。加密/解密单元402将解密的加密目标数据DR1一直保持到从应答数据产生单元407发送应答数据AD。

现在，校验和产生单元404产生所接收到的解密的加密目标数据DR1的CS2，并将其发送到校验和确定单元406（S907）。校验和确定单元406然后实现所接收的CS1和CS2的比较处理（S908）。

如果比较处理的结果是CS1=CS2，则校验和确定单元406发送告知校验和相等的控制代码，如果结果是CS1≠CS2，则发送告知校验和不相等的控制代码，这两种情况下的控制代码都发送给应答数据产生单元407。

如果应答数据产生单元407接收到一个告知校验和不相等的控制代码，它不产生任何应答数据（S909）。也可以用无意义的字节串等的填充数据来填充应答数据AD或描述一个差错码，但在这个第一实施例中，基于如果校验和不相等则不产生应答数据AD的假设进行说明。或者，也可以为，如果校验和不相等则校验和确定单元406不向应答数据产生单元407发送控制代码。

然后，应答数据产生单元407根据接收到的控制代码产生应答数据AD，并将数据发送到加密/解密单元402和校验和产生单元404

（S910）。

因为确定向第一设备101发送回正确的应答数据AD的设备至少属于相同的组，因此当由于通信差错而使得校验和不相等时可以作出相同的确定。

现在，加密/解密单元402从它维护的解密的加密目标数据DR1中提取出随机信息R1。采用这个包括会话密钥等的随机信息R1，加密/解密单元402对接收的应答数据AD加密，产生加密信息E2，并将其发送到设备间通信单元405（S911）。同时，校验和产生单元404产生所接收的应答数据AD的CS3，并将其发送到设备间通信单元405（S912）。当设备间通信单元405接收到加密信息E2和CS2时，它向第一设备101发送应答数据A-Data 2，应答数据A-Data 2至少包括加密信息E2和CS3，并具有附带的符合通信协议的消息首部等（S913）。

当包括在第一设备101中的设备间通信单元305接收到来自第二设备102的应答数据A-Data 2时，它从该数据提取出加密信息E2和CS3（S914）。然后，设备间通信单元305向加密/解密单元302发送加密信息E2，向校验和确定单元306发送CS3。

当加密/解密单元302从设备间通信单元305接收到加密信息E2时，它向随机信息产生单元301发送随机信息获取请求，并从随机信息产生单元301接收随机信息R1。然后，加密/解密单元302采用接收的随机信息R1作为密钥对接收的加密信息E2进行解密，获得解密的加密信息（此后称为“解密应答数据”）DA2，并将其发送到校验和产生单元304和校验和确定单元306（S915）。在将数据发送到校验和确定单元306时，还可以从解密应答数据DA2提取出设备标识信息并且也发送它。

现在，校验和产生单元304产生接收的解密应答数据DA2的CS4，并将其发送到校验和确定单元306（S916）。校验和确定单元306执行对接收的CS3和CS4的比较处理（S917）。

如果比较处理的结果是CS3=CS4，则确定发送应答数据AD的第二设备102属于相同组，并且将第二设备102作为一个属于相同组

的设备添加到列表中（S919）。同时，如果结果是 CS3≠CS4，则确定该设备不属于相同组，并结束处理（S918）。出于与在由第二设备 102 执行的校验和比较的结果不相等的情况下相同的原因，如果校验和由于传输错误而不相等，则作出同样的确定。这结束了对第一设备 101 和第二设备 102 之间的设备鉴别系统的详细说明。

注意，在这个第一实施例中，对于发射数据 T-Data 1 和应答数据 A-Data 2，加密目标部分分别是加密目标数据 ED 和应答数据 AD，不包括校验和 505 和校验和 605。然而，也可以实现包括校验和 505 和校验和 605 的加密。

具体地，当在第一设备 101 中创建发射数据 T-Data 1 时，在计算出校验和目标部分 CT 的校验和 505 之后，校验和目标部分 CT 和校验和 505 都可以采用公共信息 A 加密。然后，包括都被加密的校验和目标部分 CT 和校验和 505 的发射数据 T-Data 1 被发送给第二设备 102。同时，在第二设备 102 这端，采用公共信息 A 对接收的发射数据 T-Data 1 进行解密，并且在实现了指定的处理之后，可以采用随机信息 503 对加密信息 E2 和校验和 CS3 加密，然后作为应答数据 A-Data 2 发送回去。

如同已经说明的，在依据这个第一实施例的设备鉴别系统中，从第一设备 101 发送的发射数据 T-Data 1 包括包含已经采用公共信息 A 加密的随机信息 503 等的加密目标数据 ED 和校验和 505。第二设备 102 采用公共信息 A 对加密目标数据 ED 解密，并通过实现校验和 505 的比较处理来确定第一设备 101 是否属于相同组。如果第一设备 101 属于相同组，则第二设备 102 向第一设备 101 发送回应答数据 A-Data 2，应答数据 A-Data 2 包括已经采用随机信息 503 加密的加密信息 E2 和校验和 605。当第一设备 101 接收到应答数据 A-Data 2 时，它采用已经保存的随机信息 503 对应答数据 AD 解密，通过实现校验和 605 的比较处理来确定第二设备 102 是否属于相同组，并且，如果校验和相等，则将第二设备 102 添加到组列表中。

因此，在这个第一实施例的设备鉴别系统中，第一设备 101 在不向其他设备发送公共信息 A 的情况下自身能够创建属于相同组的设

备的组列表，这使得第一设备 101 在它进行将给第一设备 101 带来沉重负担的诸如鉴别处理或内容发射处理的处理之前，能够安全地获取属于相同组的设备的组列表。

另外，在这个第一实施例的设备鉴别系统中，第一设备 101 自身能够独立于服务器来创建属于相同组的设备的组列表，这在经由广播等实现多个设备间的编组是很有效的。

并且，在依据这个第一实施例的设备鉴别系统中，在将每个设备都视为与持有公共信息 A 的终端在相同级别的情况下，则通过根据上述组列表决定它将数据发送给哪个设备，每个设备不会对不被允许获得该内容的设备进行传输。这样，高效利用通信网络和减少通信量等是可能的。

此外，在这个第一实施例中，通过采用随机数的随机信息 R1 来用于应答数据 A-Data 2 的加密和解密，可以使第一设备 101 和第二设备 102 之间的数据传输更加安全，并且更有效地避免诸如重放攻击这样的攻击，重放攻击是一种通过获得先前通信的内容并将假装是该内容的发送者而发送相同内容的攻击计算机的方式。

到目前为此，在这个第一实施例中，已经说明了在设备之间发送的数据包括消息首部 501、被加密的加密目标数据 ED 和这个加密目标数据 ED 的校验和，并在接收方的第二设备 102 实现校验和的比较处理。然而，也可以使预先决定的固定信息包括在加密目标数据 ED 中，并且接收方通过检查是否包括该固定信息来判断发送设备是否持有相同的公共信息 A。在这种情况下，在设备之间发射的数据可以包括消息首部 501 和包括固定信息的加密的加密目标数据 ED。包括固定信息意思是，例如，在加密目标数据 ED 的头部插入一个诸如“Hello”之类的字母串。

并且，在这个实施例中，对于另一个设备是否属于相同组的确定是由第二设备采用公共信息 A 实现的，但可以使对于一个设备是否属于相同组的确定不由第二设备 102 实现，而仅由第一设备 101 实现。例如，第二设备 102 采用公共信息 A 对接收的加密信息 E1 解密并获取随机信息 R1 是可能的。然而，在不进行校验和确定（不判断是否

持有相同的公共信息 A）的情况下，第二设备 102 采用上述的随机信息 R1 对应答数据 AD 加密，并将其发送回第一设备 101。第一设备 101 然后对该数据解密，确定所获得的数据作为应答数据 AD 是否是正确的，因而确定发送设备是否属于相同组。

（第二实施例）

现在，说明依据本发明的第二实施例的设备鉴别系统。在这个第二实施例中，为了简化说明，将主要说明不同于第一实施例的地方。这个第二实施例与内容分发系统有关，其中，以分离的形式管理数字产品（内容）和使得用户能够利用该内容的权利信息（许可），并通过网络从服务器分发给终端。在第二实施例中，以一个用于搜索存储在相同组内的其他终端中的许可的系统为例子。

图 10 是显示依据这个第二实施例的第三设备 1001 的详细结构的方框图。在这个第二实施例中，除了上述第一设备 101 的结构之外，第三设备 1001 还包括内容使用单元 1001a、输入单元 1005 和搜索信息附加单元 1007。

内容使用单元 1001a 在经由诸如宽带的网络从服务器下载诸如电影或音乐的内容以及许可时使用。它包括存储诸如电影的内容之类的内容存储单元 1002、存储由服务器应来自作为 PC 用户等的终端的请求而发出的许可的许可存储单元 1003 以及根据由许可允许的使用规则来管理存储在内容存储单元 1002 中的内容的输出控制单元 1004。然而，内容使用单元 1001a 的结构只是一个用于说明的例子，其结构并不限制这个第二实施例。

内容存储单元 1002 存储当终端用户实行购买过程时通过宽带等从服务器下载的内容。这些内容通常在服务器采用内容密钥加密之后发送给第三设备 1001。

在许可存储单元 1003 中，存储由终端用户等获得的由服务器应用户的请求而发出的许可。许可是给予客户内容的使用允许的数据，包括诸如与许可相联系的内容的内容 ID、描述内容的使用形式的动作 ID 以及对加密内容解密的内容密钥之类的信息，此外，它还存储

指示设备上的内容使用规则的使用规则数据。在使用规则数据中，包括诸如有效期（例如，从2002年6月1日到2002年8月31日）、允许使用的最大次数（例如，允许重现一次）或每次连续重现的最大时间长度（例如，最大允许每次重现10小时）之类的信息。由服务器管理的使用规则是，例如，包括在许可中的使用规则以及可以由服务器获得并管理的信息（例如，用户的使用记录或由用户拥有的设备列表）。

输出控制单元1004具有或通过电缆连接到诸如电视、扬声器或打印机之类的重现设备，第三设备1001的用户在许可的使用允许的范围内利用这些再现设备使用内容。通过将输出控制单元1004与记录设备相连，也可以将内容记录到诸如DVD或SD的存储介质上。

输入单元1005通过网络与第三设备1001相连，向包括在第三设备1001中的内容使用单元1001a输入诸如内容、许可或用户信息之类的数据。这个输入单元1005由具有数据库的服务器一方控制。

除了第一实施例的结构之外，终端管理单元1001b还包括搜索信息附加单元1007。当第三设备1001向其他设备发送发射数据T-Data 3时的数据流如下。首先，随机信息产生单元301和搜索信息附加单元1007产生随机信息R2和搜索信息C。在这个搜索信息C中，包括关于内容ID和要搜索的许可允许使用的动作ID的信息。在这个搜索信息C中还可以包括其他信息。然后，加密/解密单元302采用公共信息A产生包括搜索信息C和随机信息R2的加密信息E3，并将这个加密信息E3发送给设备间通信单元305。同时，校验和确定单元304根据随机信息R2和搜索信息C产生CS5，设备间通信单元305将包括加密信息E3和CS5的发射数据T-Data 3发送给第四设备1101。

现在，当第三设备1001从其他设备接收应答数据A-Data 4时的数据流如下。首先，在从第四设备1101接收到的应答数据A-Data 4中，设备间通信单元305将加密数据E4发送给加密/解密单元302用于解密，同时将CS7发送给校验和确定单元306。加密/解密单元302然后采用它正维护的随机信息R2对数据E4解密，并将这个解密应答数据DA4发送给校验和产生单元304。当校验和确定单元306接

收到由校验和产生单元304产生的CS8时，它将CS7与CS8进行比较，如果比较结果是CS7与CS8相等，则将运用于搜索信息C并由第四设备1101持有的许可信息添加到由第三设备1001创建的许可列表中。

图11是显示依据第二实施例的第四设备1101的详细结构的方框图。与上述的第三设备1001类似，第四设备1101包括内容使用单元1101a、输入单元1105和终端管理单元1101b。内容使用单元1101a的结构与上述的内容使用单元1001a类似。

除了第一实施例中的结构之外，终端管理单元1101b还包括搜索信息确定单元1106。从终端管理单元1101b接收到发射数据T-Data 3直到它发送出一个响应这段时间的数据流如下。首先，设备间通信单元405接收发射数据T-Data 3，并将加密信息E3发送给加密/解密单元402，将CS5发送给校验和确定单元406。加密/解密单元402采用公共信息A对加密信息E3解密，将解密的加密目标数据DR2发送给校验和产生单元404，在那里产生的CS6被发送给校验和确定单元406。校验和确定单元406然后比较CS5和CS6。如果结果是校验和不相等，则忽略发射数据T-Data 3，但如果校验和相等，则搜索信息确定单元1106搜索内容使用单元1101a并检索出对应于适用于搜索信息C的内容的许可。如果未找到满足搜索信息C的许可，则应答数据产生单元407不创建任何应答数据AD，但如果找到满足搜索信息C的许可，则创建包括许可信息C2和应答数据AD的加密信息E4。然后，设备间通信单元405向第三设备1001发送包括加密信息E4以及根据许可信息C2和应答数据AD产生的CS7的应答数据A-Data 4。

图12是显示依据这个第二实施例的发射数据T-Data 3的数据结构的示意图。注意，图12只是一个说明第二实施例的例子。

发射数据T-Data 3是一个请求其他设备确定它们是否与第三设备1001属于相同组以及搜索应用于搜索信息的许可的的消息。除了在第一实施例中说明的发射数据T-Data 1的结构之外，它还包括关于内容ID 1201和动作ID 1202的数据。

内容 ID 1201 指示所请求内容的 ID。对于任何内容，每个内容至少分配一个标识符以唯一地标识该内容，通常，这个标识符用作内容 ID 1201。内容 ID 1201 是与要搜索的许可相对应的内容的 ID。

动作 ID 1202 是指定由上述内容 ID 1201 指示的内容的使用形式的标识符，也是要搜索的许可所允许的动作的 ID。在这种情况下，动作包括听、再现、复制、移动或打印。

内容 ID 1201 和动作 ID 1202 包括在发送之前由公共信息 A 加密的加密目标数据 ED 之内。与第一实施例类似，在第二实施例中，也可以在发送之前不仅采用公共信息 A 对加密目标数据 ED 加密，还采用公共信息 A 对校验和 505 加密。

图 13 是显示依据第二实施例的应答数据 A-Data 4 的数据结构的示意图。这个应答数据 A-Data 4 是对已经从第三设备 1001 发送的发射数据 T-Data 3 的响应，除了第一实施例的应答数据 A-Data 2 的结构之外，它还包括许可 ID 1301 和使用规则数据 1302。

许可 ID 1301 自身不是一个许可，即权利信息，而是可以用于搜索信息 C 的内容的许可的标识号，在这个第二实施例中，它是用于标识一个在第四设备 1101、即进行搜索的终端中被搜索的许可的数字。

使用规则数据 1302 是指示由许可允许的内容的使用规则的数据，通常包括在许可中。在这个第二实施例中，它包括诸如 C 规则的信息，C 规则确定是否可以在由第三设备 1001 确定的规则下（例如，十次）开始一个动作-内容的操作，例如听。

许可 ID 1301 和使用规则数据 1302 都包括在由随机信息 R2 加密的应答数据 AD 中。

图 14 是显示依据第二实施例的当第三设备 1001 采用搜索信息 C 实现为第四设备 1101 和第五设备 1401 的许可搜索时的传输过程的时序图。注意，在这个图中，假设第五设备 1401 不持有公共信息 A。

第三设备 1001 搜索存储在属于相同组的其他终端中的许可，并创建持有包括在搜索信息 C 中的内容的许可的设备的许可列表。为了实现这个处理，第三设备 1001 向第四设备 1101 和第五设备 1401

发送包括搜索信息 C 的由公共信息 A 加密的发射数据（S1402）。在这个实施例中，通过广播进行发射。

当第四设备 1101 和第五设备 1401 接收到发射数据时，它们采用公共信息 A 对发射数据的数据的加密部分进行解密，并进行校验和比较（S1403）。虽然第五设备 1401 接收到发射数据，但因为它未持有公共信息 A，因此不能正确地实现对加密的发射数据的解密，导致校验和不相等，因而不发送回任何应答数据（S1404）。

同时，第四设备 1101 确定是否满足公共信息 A 以及搜索信息 C（S1405），如果满足它们，则发送回附带有许可信息的应答数据（S1407），但如果不满足它们，则不发送回响应（S1406）。然后，如图 14 所示，第三设备 1001 创建满足搜索信息 C 的许可列表 1408，并根据这个许可列表 1408 确定它将向哪些设备发送数据。

图 15 是显示依据第二实施例的设备鉴别系统中的组确定过程的流程图。已经采用图 9 说明了依据第一实施例的设备鉴别系统的组确定过程，对于与第一实施例类似的步骤，在图 15 中同样采用与图 9 相同的步骤标号。根据图 15 说明第三设备 1001 创建与它自身属于相同组并满足搜索信息 C 的设备的许可列表 1408 的详细流程。

首先，包括在第三设备 1001 中的随机信息产生单元 301 产生随机信息 R2（S901），搜索信息附加单元 1007 产生包括要搜索的内容的内容 ID 1201 和动作 ID 1202 的搜索信息 C（S1501）。然后，将随机信息 R2 和搜索信息 C 发送到加密/解密单元 302 和校验和产生单元 304。

当加密/解密单元 302 从随机信息产生单元 301 接收到随机信息 R2 时，它向公共信息存储单元 303 发送公共信息获取请求，并从公共信息存储单元 303 接收公共信息 A。然后，加密/解密单元 302 采用公共信息 A 作为密钥对至少包括随机信息 R2 和搜索信息 C 的加密目标数据 ED 进行加密，产生加密信息 E3 并将其发送到设备间通信单元 305（S902）。

接着，校验和产生单元 304 产生至少包括随机信息 R2 和搜索信息 C 的加密目标数据 ED 的 CS5，并将其发送到设备间通信单元 305

（S903）。

当设备间通信单元 305 接收到加密信息 E3 和 CS5 时，它将发射数据 T-Data 3 发送给其他设备，发射数据 T-Data 3 至少包括加密信息 E3 和 CS5 并且还附带有符合通信协议的消息首部等（S904）。

下面，当包括在第四设备 1101 中的设备间通信单元 405 从第三设备 1001 接收到发射数据 T-Data 3 时，它从发射数据 T-Data 3 提取出上述的加密信息 E3 和 CS5（S905）。然后，设备间通信单元 405 将加密信息 E3 发送给加密/解密单元 402，将 CS5 发送给校验和确定单元 406。

在加密/解密单元 402 接收到加密信息 E3 之后，它从公共信息存储单元 403 接收公共信息 A。加密/解密单元 402 采用这个公共信息 A 作为密钥对加密信息 E3 进行解密，获得解密的加密目标数据 DR2，并将其发送到校验和产生单元 404（S906）。接着，校验和产生单元 404 产生所接收到的解密的加密目标数据 DR2 的 CS6，并将其发送给校验和确定单元 406（S907）。然后，校验和确定单元 406 实现所接收的 CS5 和 CS6 的比较处理（S908）。

作为比较结果，如果 CS5=CS6，则校验和确定单元 406 发送告知校验和相等的控制代码，如果 CS5≠CS6，则发送告知校验和不相等的控制代码，这两种情况下的控制代码都发送给应答数据产生单元 407。然后，如果应答数据产生单元 407 接收到告知校验和不相等的控制代码，则不产生任何应答数据（S909）。

下面，搜索信息确定单元 1106 确定该设备是否持有可以被用于适用于从第三设备 1001 发送的发射数据 T-Data 3 的搜索信息 C 的内容 ID 的任何许可，如果持有任何相关的许可，则该设备发送回附带有许可信息 C2 的应答数据 A-Data 4（S1502）。同时，在不满足搜索信息 C 的情况下，则在不发回响应的假设下在这个第二实施例中进行说明（S1503）。然而，也可以在应答数据 A-Data 4 中描述告知未找到对应于搜索信息 C 的数据的数据。

接着，搜索信息确定单元 1106 产生包括许可 ID 等的许可信息 C2（S1504），当应答数据产生单元 407 接收到控制代码时，它根据

控制代码产生包括许可信息 C2 的应答数据 AD，并将其发送给加密/解密单元 402 和校验和产生单元 404（S910）。

加密/解密单元 402 然后从它正维护的解密的加密目标数据 DR2 中提取出随机信息 R2，并采用这个随机信息 R2 作为密钥，对接收的许可信息 C2 和应答数据 AD 加密，产生加密信息 E4，并将其发送到设备间通信单元 405（S911）。同时，校验和产生单元 404 产生所接收的应答数据 AD 的 CS7，并将其发送到设备间通信单元 405（S912）。然后，设备间通信单元 405 向第三设备 1001 发送应答数据 A-Data 4，应答数据 A-Data 4 至少包括加密信息 E4 和 CS7，并具有附带的符合通信协议的消息首部等（S913）。

现在，包括在第三设备 1001 中的设备间通信单元 305 接收到来自第四设备 1101 的 A-Data 4，并提取出加密信息 E4 和 CS7（S914）。然后，设备间通信单元 305 向加密/解密单元 302 发送加密信息 E4，向校验和确定单元 306 发送 CS7。

当加密/解密单元 302 从设备间通信单元 305 接收到加密信息 E4 时，它从随机信息产生单元 301 接收随机信息 R2。然后，加密/解密单元 302 采用随机信息 R2 作为密钥对接收的加密信息 E4 进行解密，获得解密的加密信息（此后称为“解密应答数据”）DA4，并将其发送到校验和产生单元 304 和校验和确定单元 306（S915）。校验和产生单元 304 产生接收的解密应答数据 DA4 的 CS8，并将其发送到校验和确定单元 306（S916）。然后，校验和确定单元 306 进行对接收的 CS7 和 CS8 的比较处理（S917）。

如果比较的结果是 CS7=CS8，则校验和确定单元 306 确定发送应答数据 AD 的第四设备 1101 属于相同组，并且该设备还具有对应于要检索的内容的许可，因此将由第四设备 1101 持有的并要检索的许可添加到许可列表 1408 中（S1505）。如果是 CS7≠CS8 的情况，则确定发送设备或者不属于相同组，或者不满足搜索信息 C（S918）。在这个第二实施例中，发射数据 T-Data 3 和应答数据 A-Data 4 的加密目标部分分别是加密目标数据 ED 和应答数据 AD。然而，也可以将校验和 505 和校验和 605 包括在加密部分中。

如同已经说明的，在依据第二实施例的设备鉴别系统中，由第三设备 1001 发送的发射数据 T-Data 3 除了随机信息 503 之外，还包括作为搜索信息 C 的内容 ID 1201 和动作 ID 1202。第四设备 1101 采用公共信息 A 对加密的加密目标数据 ED 进行解密，通过比较校验和 505 来确定第三设备 1001 是否属于相同组，如果第三设备 1001 属于相同组，在搜索信息确定单元 1106 进一步确定设备是否持有对应于要搜索的内容 ID 1201 和动作 ID 1202 的内容的许可。作为确定的结果，如果设备持有满足搜索信息 C 的许可，则向第三设备 1001 发回包括诸如许可 ID 1301 和使用规则数据 1302 的信息的应答数据 A-Data 4。

当第三设备 1001 接收到应答数据 A-Data 4 时，它采用随机信息 503 对应答数据 AD 解密，并通过执行校验和 605 的比较处理来确定第四设备 1101 属于相同组并且还持有满足搜索信息 C 的许可，从而创建满足搜索信息 C 的许可列表 1408。

因此，除了在第一实施例中描述的积极效果之外，在这个第二实施例中的设备鉴别系统不是使经由广播从第三设备 1001 接收到发射数据 T-Data 3 的所有设备而是仅仅使属于相同组的并且还持有满足搜索信息 C 的许可的那些设备发送回应答数据 A-Data 4。这样，第三设备 1001 创建许可列表 1408、即持有经过检索的许可的设备的列表，并可以根据许可列表 1408 更有效地确定例如可以交换或购买许可的设备。因此，本发明可以运用于内容分发系统中的设备之间的许可搜索。

在上述每个实施例中，采用公共信息 A 来对公共信息作出解释。然而，也可以使每个设备持有多个公共信息，并且它通过例如添加或删除多个公共信息能够灵活并容易地设置组的范围。

从上面的解释可以明显看出的，依据本发明的设备鉴别系统至少包括第一设备和用于确定第一设备与其是否属于相同组的第二设备，其中，第一设备包括：第一公共信息存储单元，用于存储公共信息；发射数据产生单元，用于产生包括密钥信息的发射数据；第一加密单元，用于采用公共信息对产生的发射数据进行加密；第一发射单元，

用于将第一加密单元产生的加密发射数据发送给第二设备；第一解密单元，用于采用密钥信息对从第二设备发送的加密应答数据进行解密；以及，鉴别单元，用于判断解密应答数据是否具有一个预定规则，当解密应答数据具有一个预定规则时，确定第一设备和第二设备属于相同组，以及，第二设备包括：第二公共信息存储单元，用于存储公共信息；第二解密单元，用于采用公共信息对从第一设备发送的加密发射数据进行解密；判断单元，用于判断解密发射数据是否具有一个预定规则；应答数据产生单元，用于当发射数据具有一个预定规则时，确定第一设备和第二设备属于相同组，并产生指示第一设备和第二设备属于相同组的应答数据；第二加密单元，用于采用在由第二解密单元解密的发射数据中包括的密钥信息对产生的应答数据进行加密；以及，第二发射单元，用于将第二加密单元产生的加密应答数据发送给第一设备。

以这种方式，依据本发明的设备鉴别系统使当终端彼此具有平等的关系时一个终端能够确定属于相同组的其他终端，并在它进行诸如鉴别或内容传输等给予终端沉重负担的处理之前使一个终端能够以安全的方式获得属于相同组的设备的列表。此外，通过采用上述的组列表，设备鉴别系统使一个终端能够确定它将向哪个设备发送发射数据，并通过不与那些不被允许获得特定内容的终端进行通信来实现通信信道等的有效利用。

并且，在依据本发明的设备鉴别系统中，发射数据产生单元产生包括指定搜索目标的搜索信息的发射数据，第二设备进一步包括搜索信息判断单元，用于判断第二设备是否保存有由解密发射数据中包括的搜索信息所指示的目标，以及，应答数据产生单元产生包括由搜索信息判断单元作出的判断的结果的应答数据。此外，发射数据产生单元使得一个指定数字内容的内容 ID 作为搜索信息被包括在发射数据中，以及，当第二设备持有许可时，应答数据产生单元使得一个指定许可的许可 ID 被包括在应答数据中，其中许可是允许利用由在发射数据中包括的内容 ID 所指示的数字内容的权利信息。

以这种方式，依据本发明的设备鉴别系统使一个终端能够创建许

可列表、即持有经过检索的许可的设备的列表，并且，该系统根据许可列表使一个终端能够更有效地确定例如可以交换或购买许可的设备，从而使得系统能够被运用于内容分发系统中的设备之间的许可搜索。

工业实用性

通过采用带有通信设备的个人计算机，依据本发明的设备鉴别系统可以应用于经由网络将内容从服务器分发到终端的内容分发系统上。

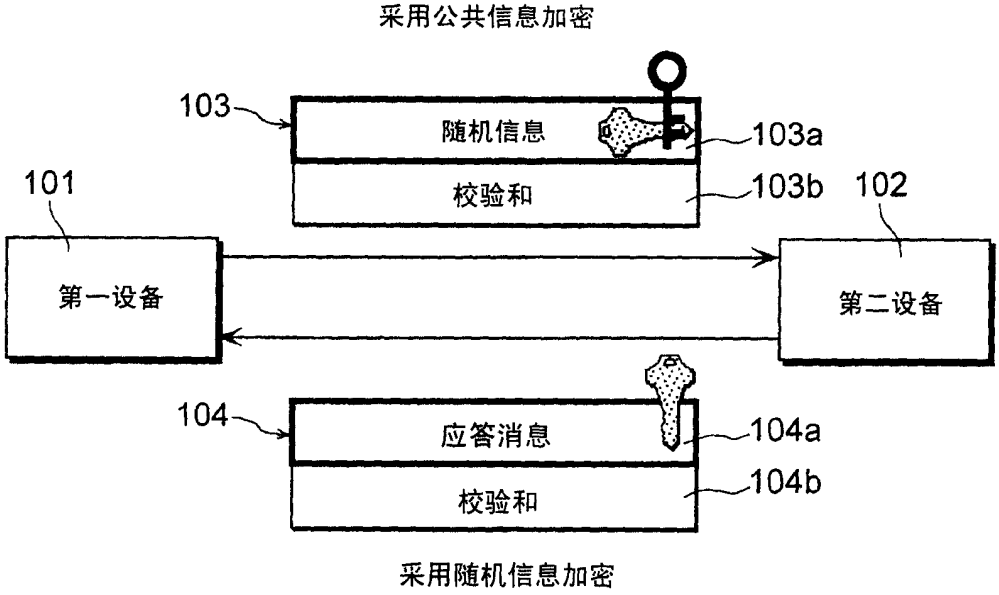

采用公共信息加密
103
随机信息
103a
校验和
103b
101
102
第一设备
第二设备
104
应答消息
104a
校验和
104b
采用随机信息加密

图1

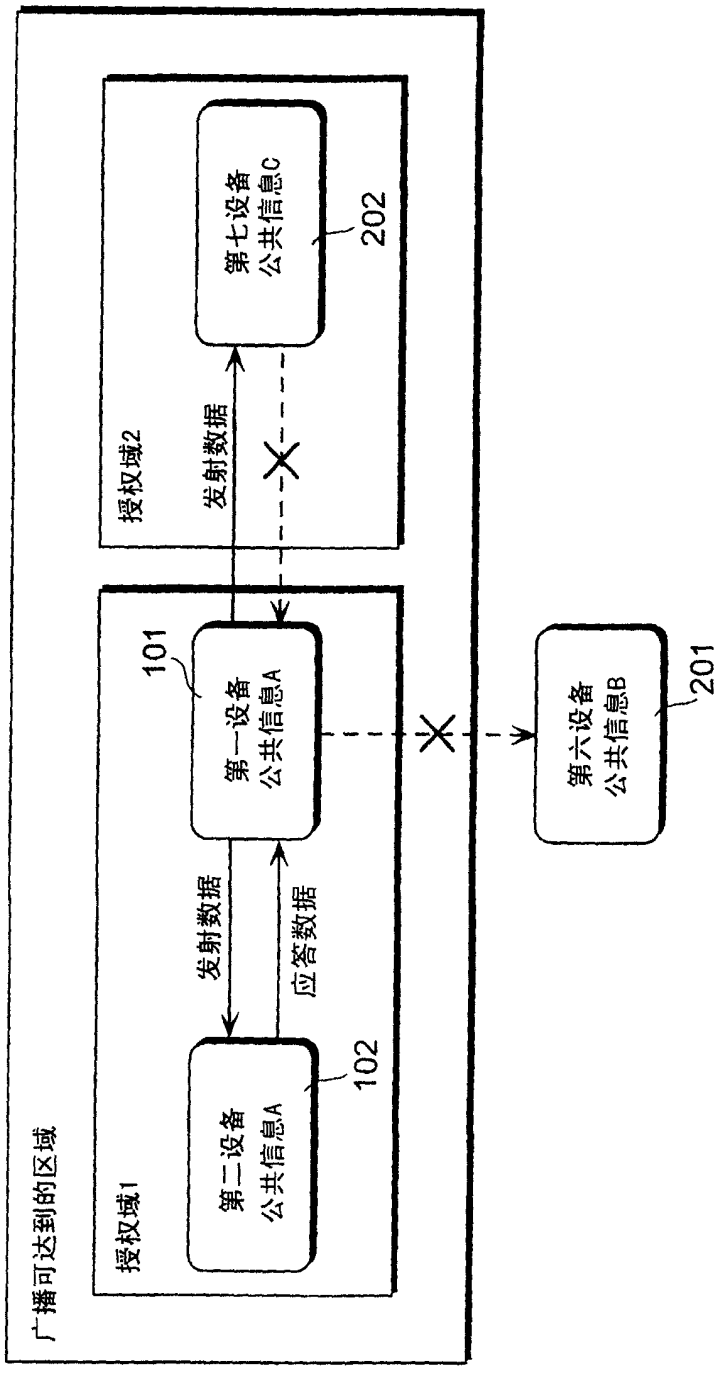

广播可达到的区域
授权域1
第二设备
公共信息A
102
发射数据
应答数据
101
第一设备
公共信息A
授权域2
发射数据
第七设备
公共信息C
202
第六设备
公共信息B
201

图2

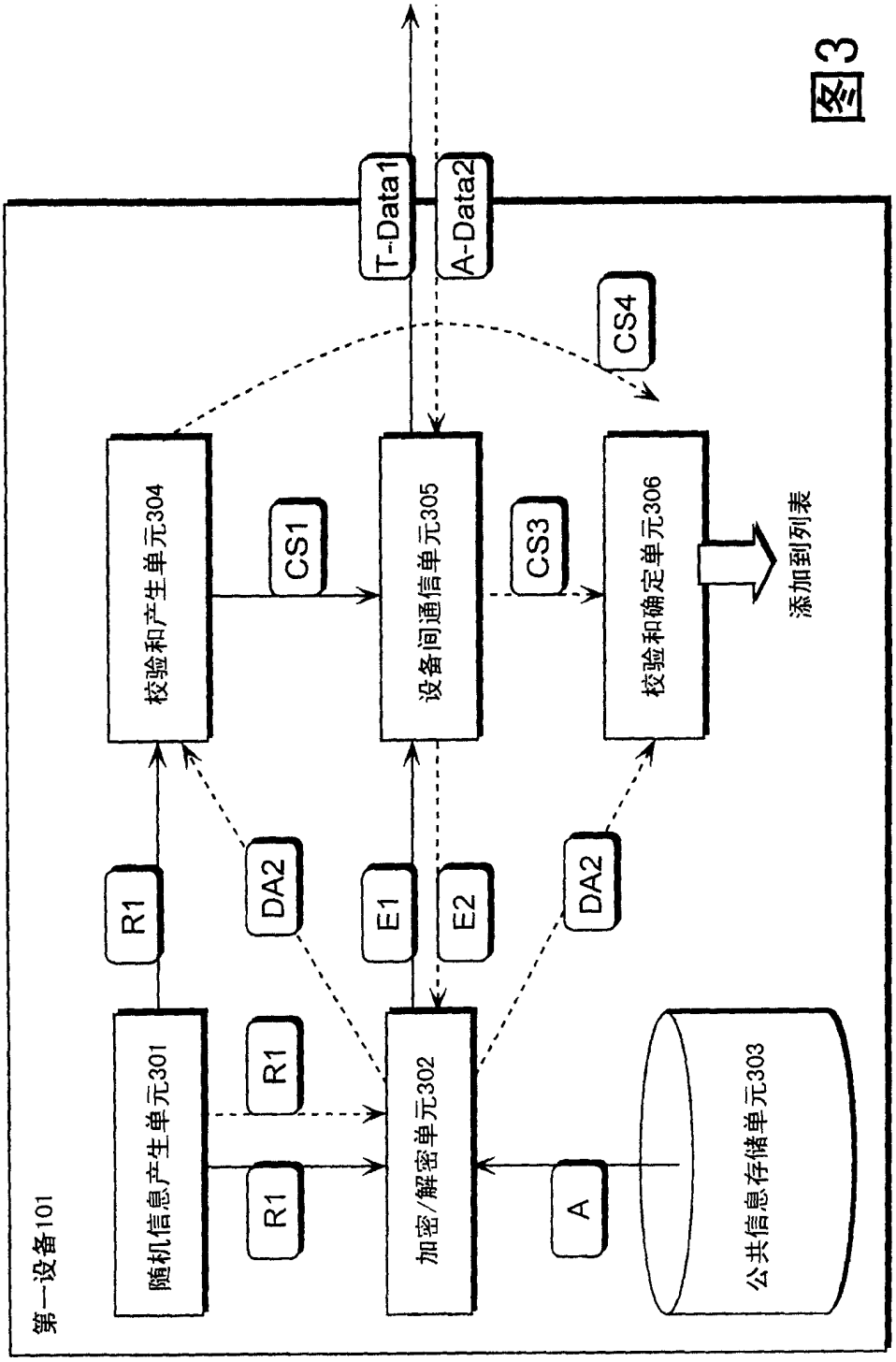

第一设备101
随机信息产生单元301
加密/解密单元302
公共信息存储单元303
校验和产生单元304
设备间通信单元305
校验和确定单元306
添加到列表
R1
R1
R1
DA2
DA2
E1
E2
A
CS1
CS3
CS4
T-Data1
A-Data2

图3

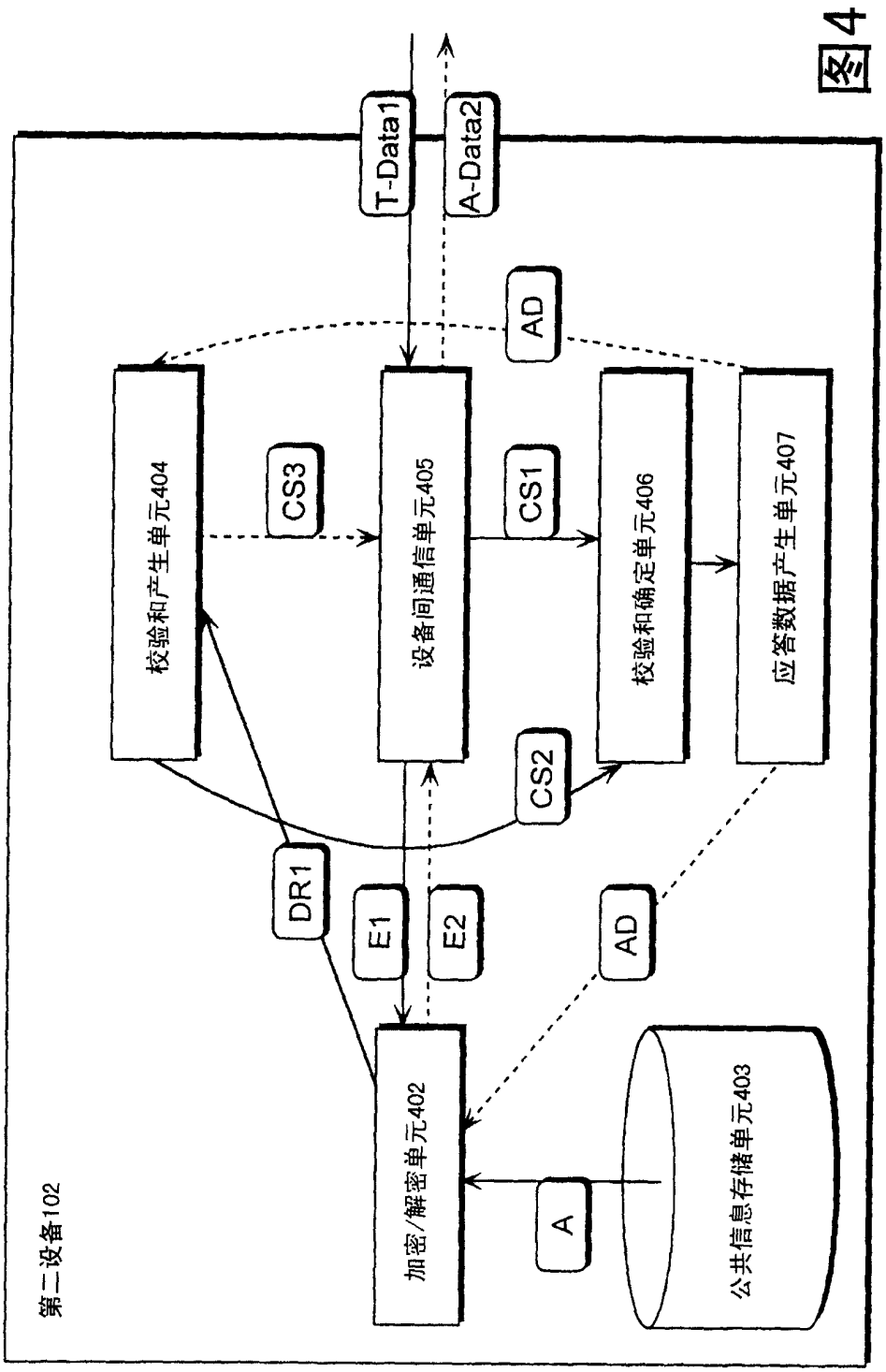

第二设备102
T-Data1
A-Data2
AD
校验和产生单元404
CS3
设备间通信单元405
CS1
校验和确定单元406
应答数据产生单元407
CS2
DR1
E1
E2
AD
加密/解密单元402
A
公共信息存储单元403

图4

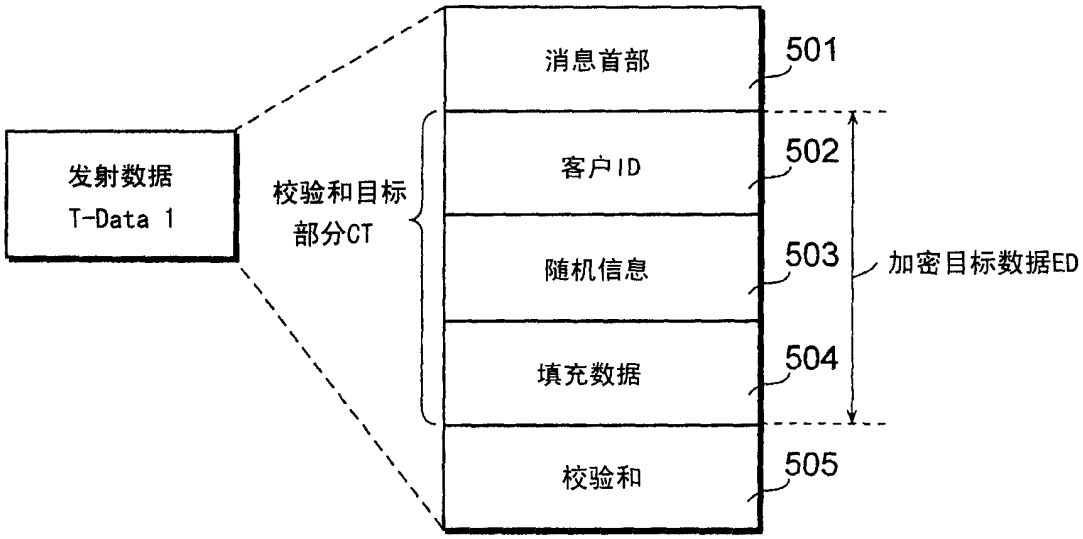

发射数据
T-Data 1
校验和目标
部分CT
消息首部
客户ID
随机信息
填充数据
校验和
501
502
503
504
505
加密目标数据ED

图5

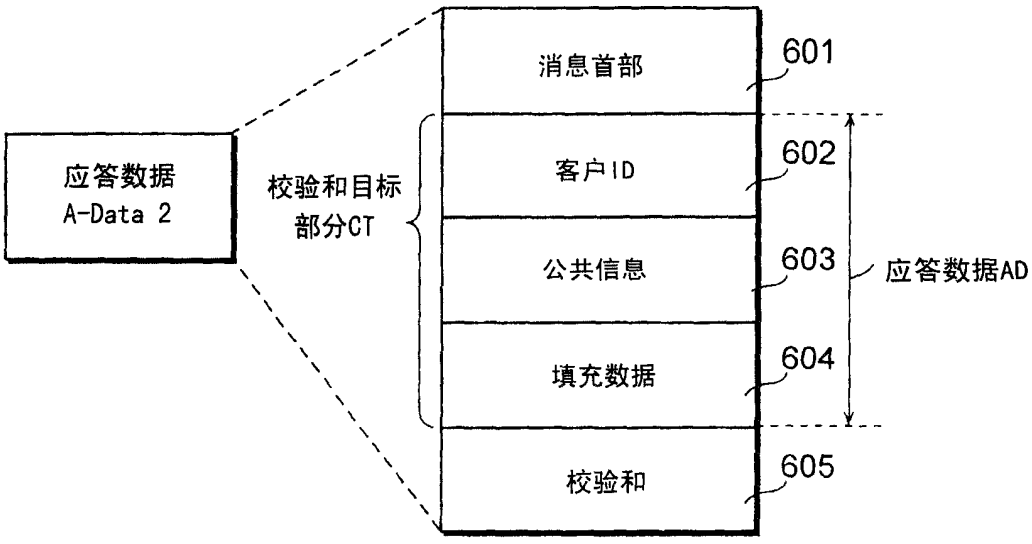

应答数据
A-Data 2
校验和目标
部分CT
消息首部
客户ID
公共信息
填充数据
校验和
601
602
603
604
605
应答数据AD

图6

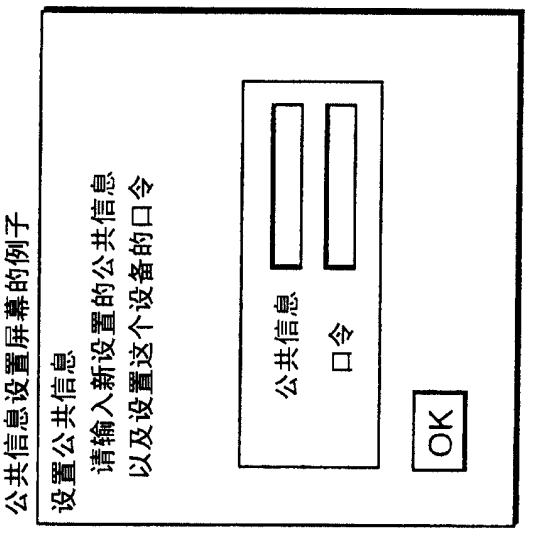

公共信息设置屏幕的例子
设置公共信息
请输入新设置的公共信息
以及设置这个设备的口令
公共信息
口令
OK

图7A

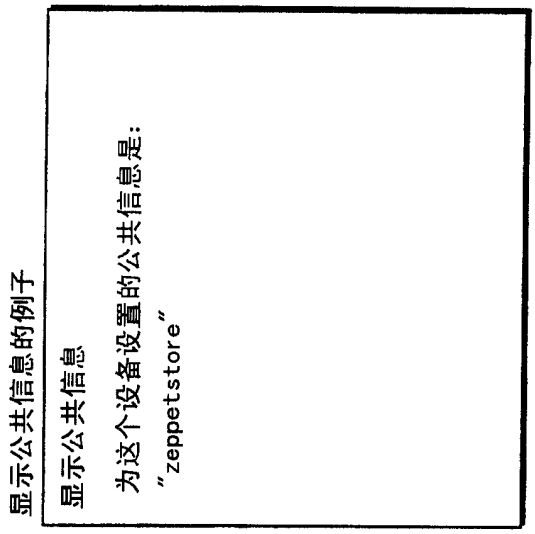

显示公共信息的例子
显示公共信息
为这个设备设置的公共信息是:
"zeppetstore"

图7B

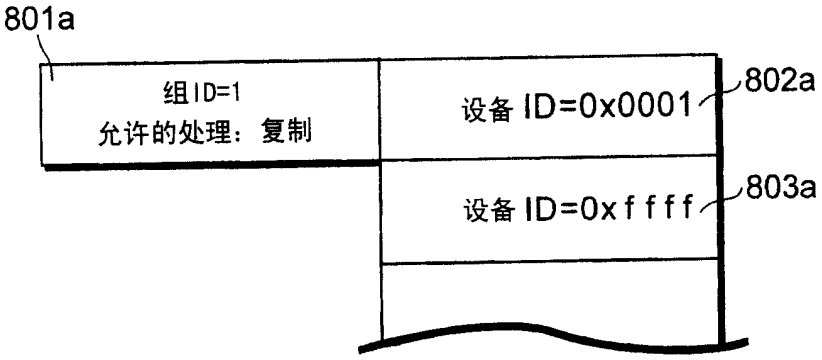

801a
组ID=1
允许的处理：复制
设备 ID=0x0001
802a
设备 ID=0xffff
803a

图8A

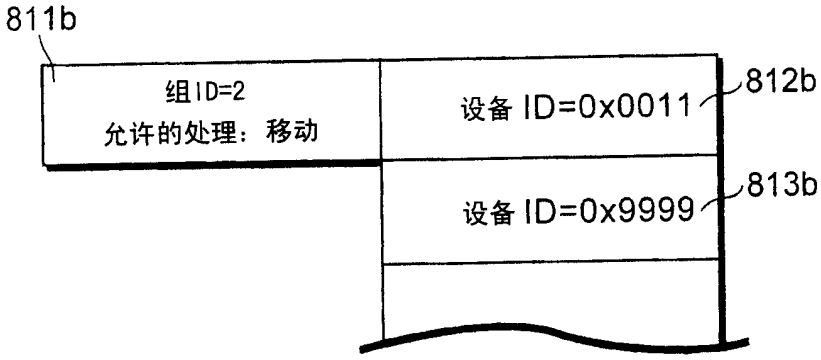

811b
组ID=2
允许的处理：移动
设备 ID=0x0011
812b
设备 ID=0x9999
813b

图8B

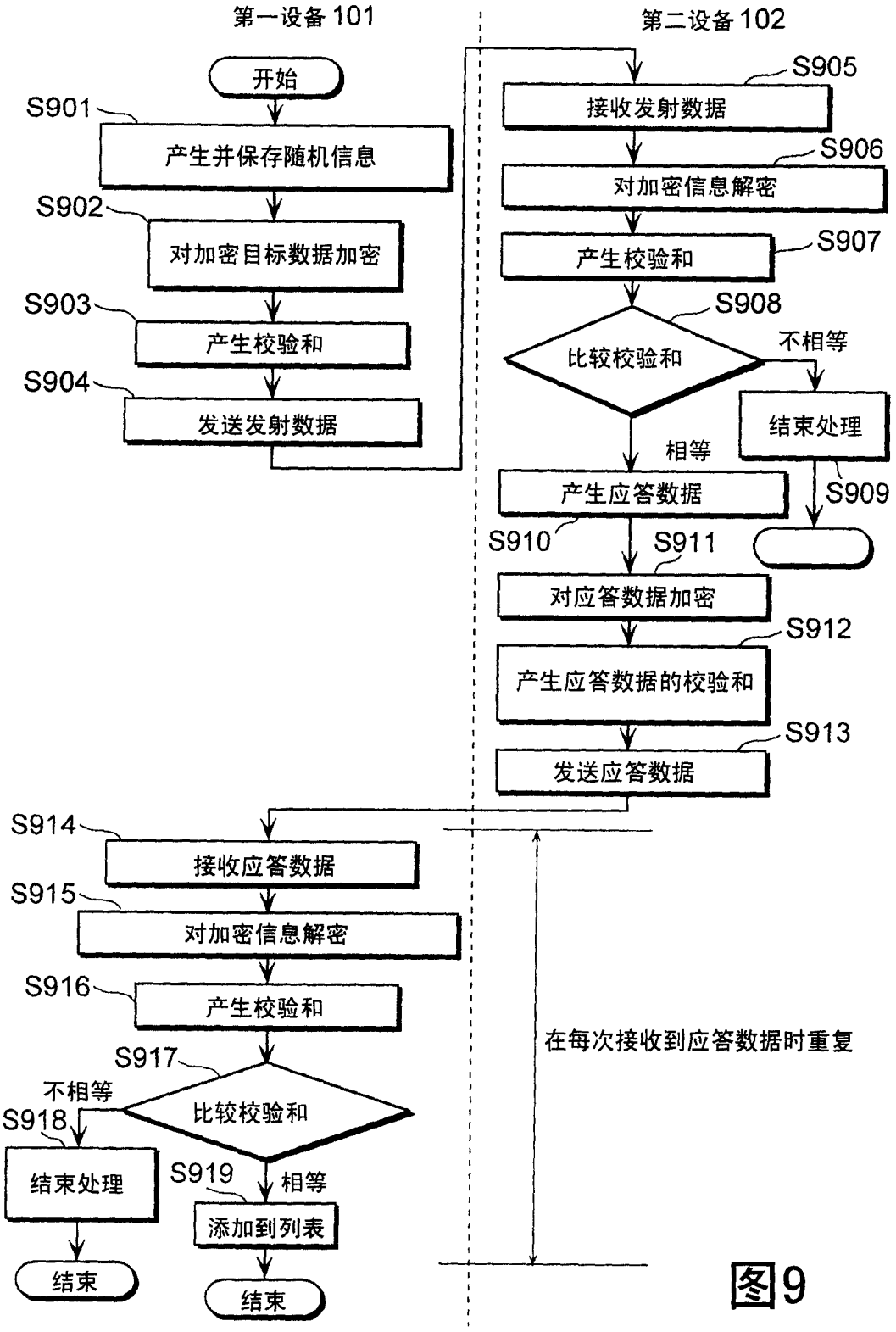

第一设备101
第二设备102
开始
S901
产生并保存随机信息
S902
对加密目标数据加密
S903
产生校验和
S904
发送发射数据
S905
接收发射数据
S906
对加密信息解密
S907
产生校验和
S908
比较校验和
不相等
结束处理
S909
相等
产生应答数据
S910
S911
对应答数据加密
S912
产生应答数据的校验和
S913
发送应答数据
S914
接收应答数据
S915
对加密信息解密
S916
产生校验和
S917
比较校验和
不相等
S918
结束处理
结束
S919
相等
添加到列表
结束
在每次接收到应答数据时重复

图9

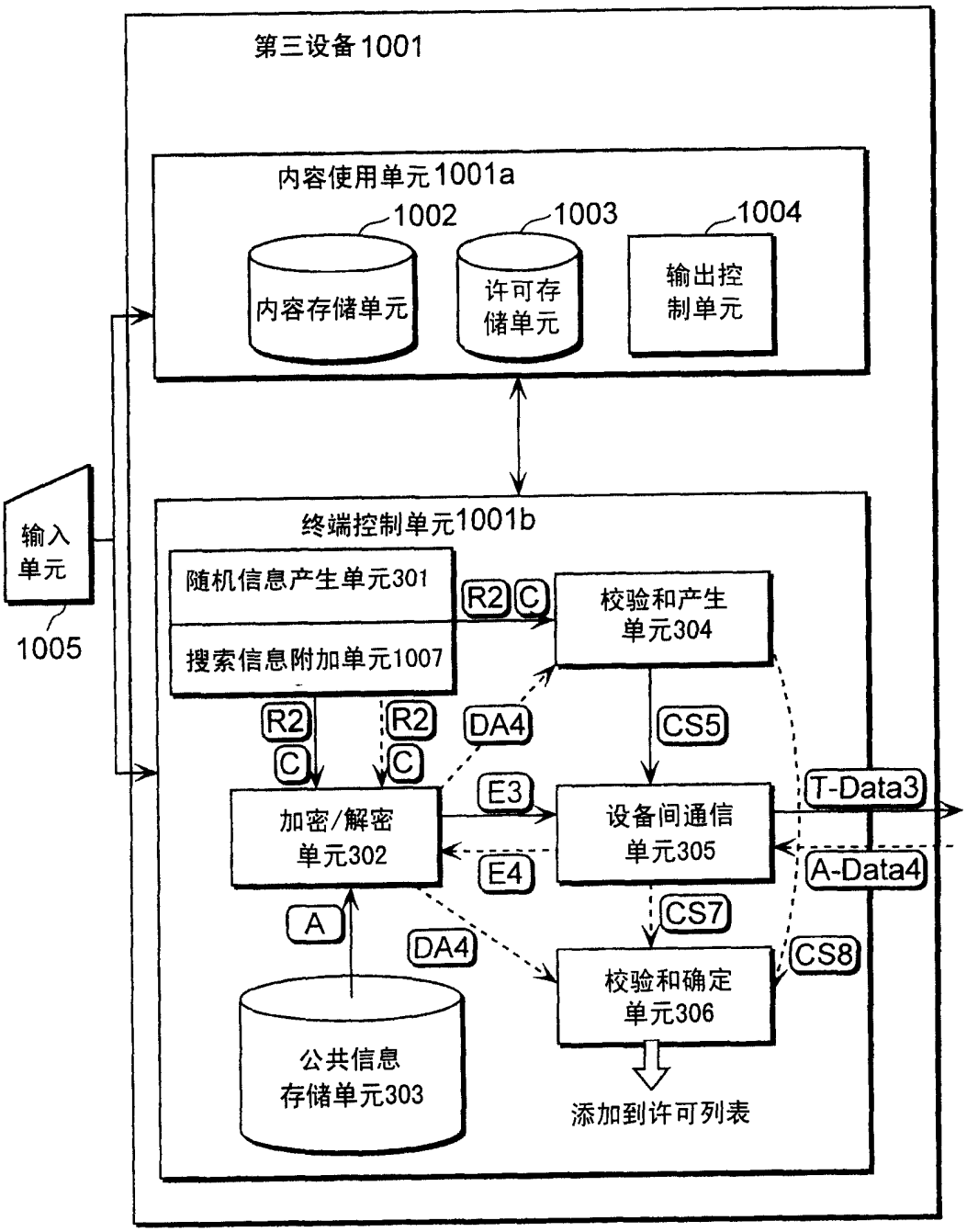

第三设备1001
内容使用单元1001a
1002
1003
1004
内容存储单元
许可存储单元
输出控制单元
终端控制单元1001b
输入单元
1005
随机信息产生单元301
搜索信息附加单元1007
R2
C
校验和产生单元304
DA4
CS5
E3
T-Data3
加密/解密单元302
设备间通信单元305
E4
A-Data4
A
CS7
DA4
CS8
校验和确定单元306
公共信息存储单元303
添加到许可列表

图10

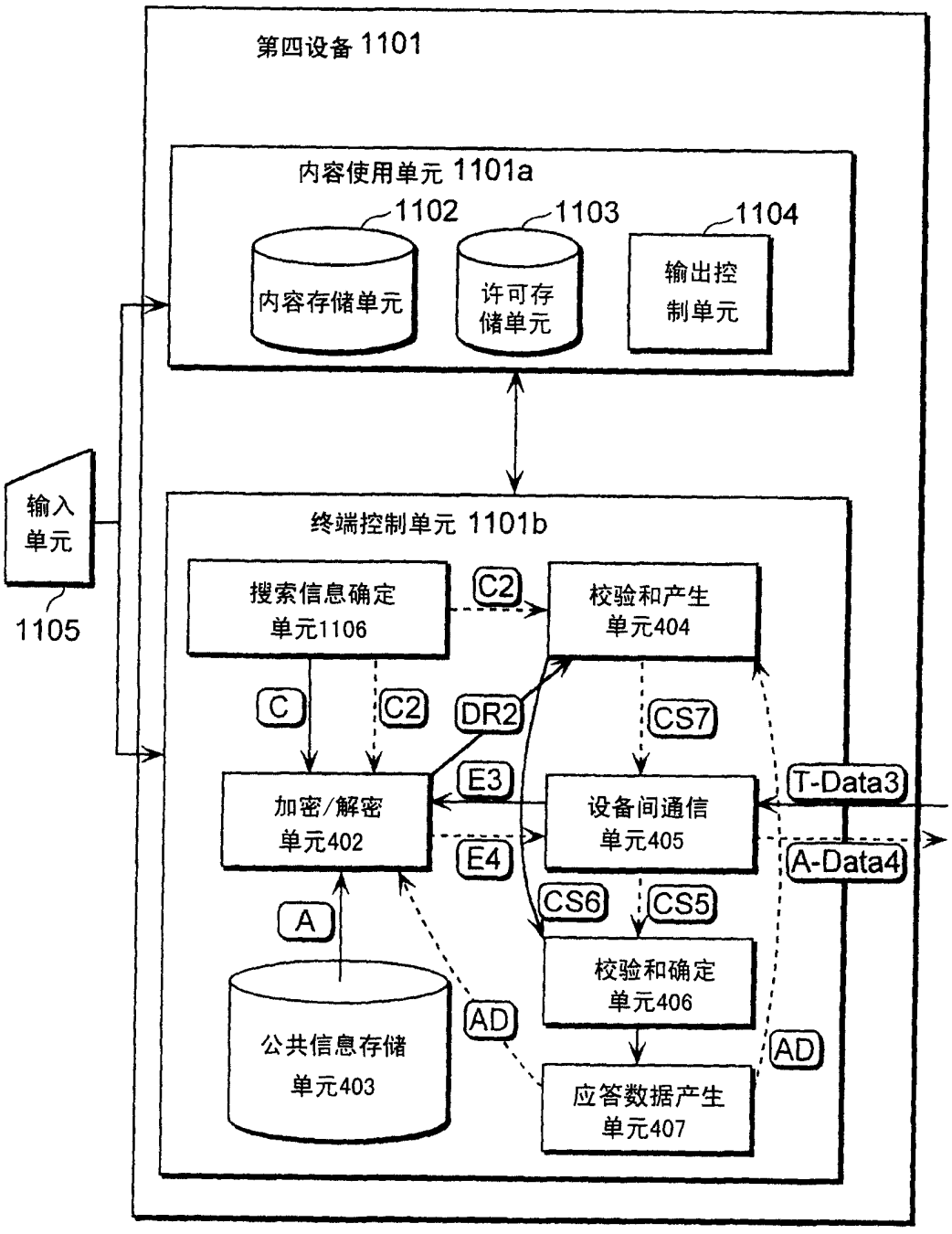

第四设备 1101
内容使用单元 1101a
1102
1103
1104
内容存储单元
许可存储单元
输出控制单元
输入单元
1105
终端控制单元 1101b
搜索信息确定单元1106
C2
校验和产生单元404
C
C2
DR2
CS7
E3
T-Data3
加密/解密单元402
设备间通信单元405
E4
A-Data4
CS6
CS5
A
校验和确定单元406
AD
AD
公共信息存储单元403
应答数据产生单元407

图11

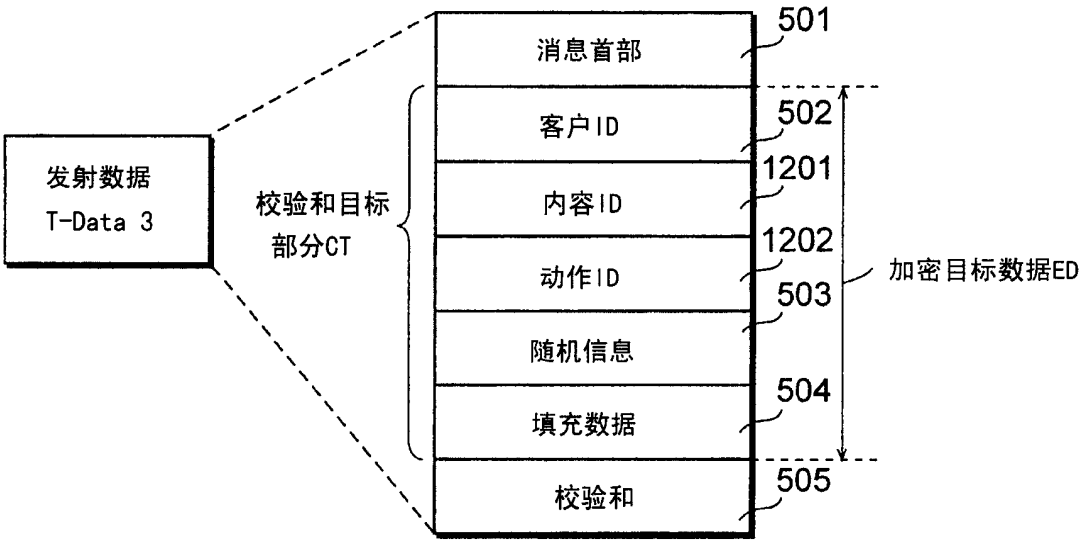

发射数据
T-Data 3
校验和目标
部分CT
消息首部
客户ID
内容ID
动作ID
随机信息
填充数据
校验和
501
502
1201
1202
503
504
505
加密目标数据ED

图12

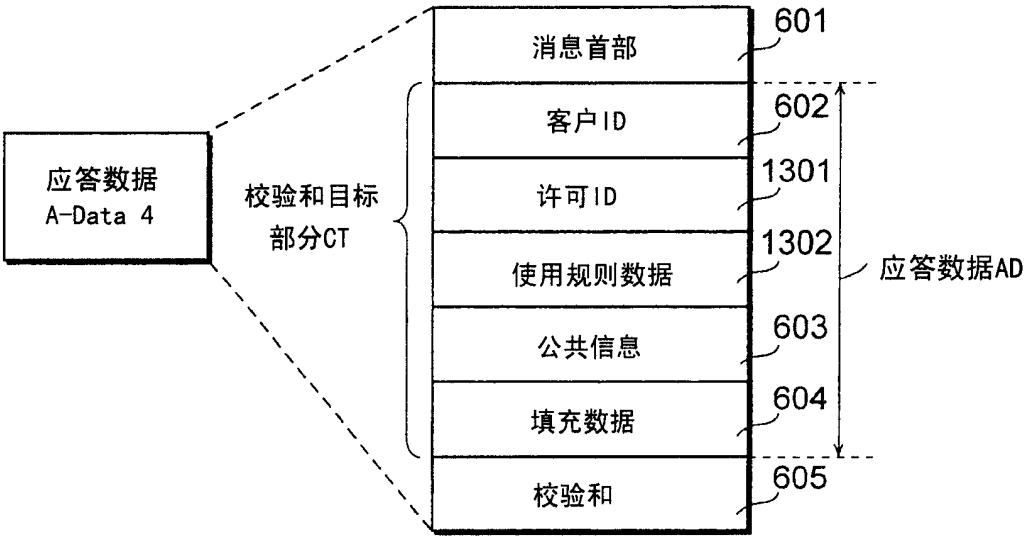

应答数据
A-Data 4
校验和目标
部分CT
消息首部
客户ID
许可ID
使用规则数据
公共信息
填充数据
校验和
601
602
1301
1302
603
604
605
应答数据AD

图13

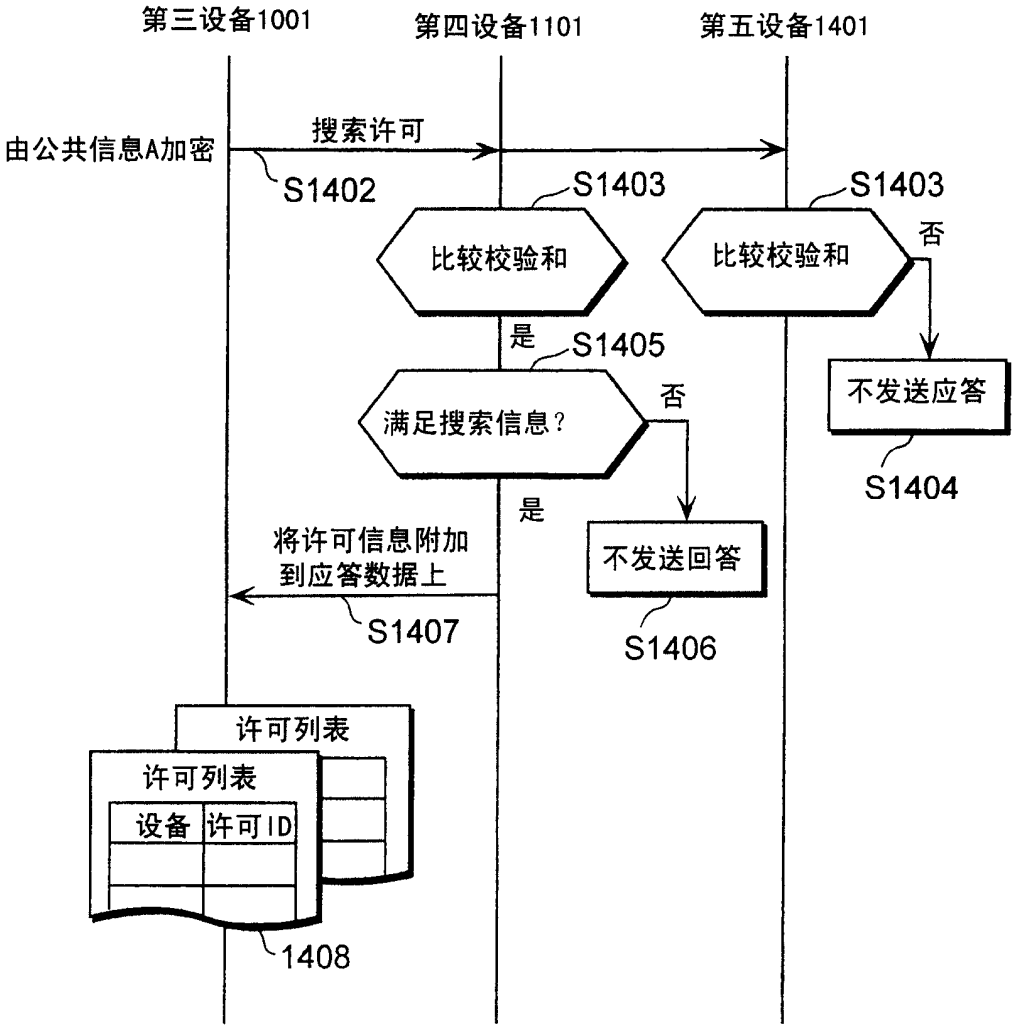

第三设备1001
第四设备1101
第五设备1401
由公共信息A加密
搜索许可
S1402
S1403
比较校验和
S1403
比较校验和
否
是
S1405
满足搜索信息？
否
不发送应答
S1404
是
将许可信息附加
到应答数据上
S1407
不发送回答
S1406
许可列表
许可列表
设备
许可ID
1408

图14

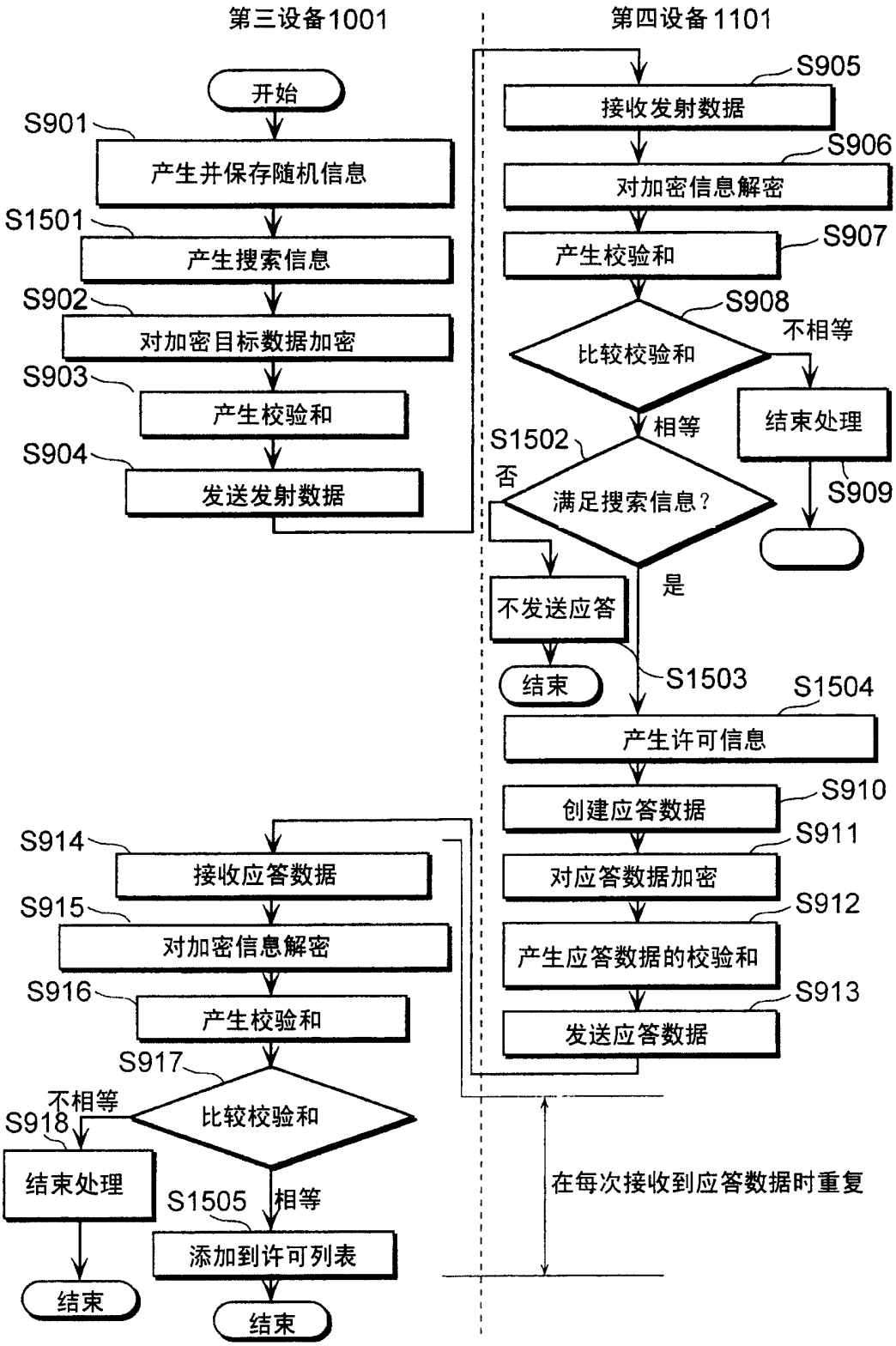

第三设备1001
第四设备1101
开始
S901
产生并保存随机信息
S1501
产生搜索信息
S902
对加密目标数据加密
S903
产生校验和
S904
发送发射数据
S905
接收发射数据
S906
对加密信息解密
S907
产生校验和
S908
比较校验和
不相等
结束处理
S909
相等
S1502
否
满足搜索信息？
是
不发送应答
结束
S1503
S1504
产生许可信息
S910
创建应答数据
S911
对应答数据加密
S912
产生应答数据的校验和
S913
发送应答数据
S914
接收应答数据
S915
对加密信息解密
S916
产生校验和
S917
比较校验和
不相等
S918
结束处理
结束
S1505
相等
添加到许可列表
结束
在每次接收到应答数据时重复

图15