(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101162495 B
(45)授权公告日 2012.04.25

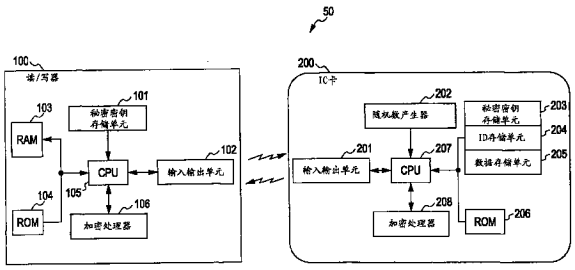
(21)申请号 200710192941.X
(22)申请日 2007.05.14
(30)优先权数据
133774/06 2006.05.12 JP
205702/06 2006.07.28 JP
(73)专利权人 索尼株式会社
地址 日本东京都
(72)发明人 森田直 金本俊范
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 郭定辉 黄小临
(51)Int.Cl.
G06K 7/00(2006.01)
H04L 9/14(2006.01)
(56)对比文件
WO 03/107585 A1,2003.12.24, 全文.
JP 10-79728 A,1998.03.24, 全文.
CN 1692566 A,2005.11.02, 全文.
CN 1465007 A,2003.12.31, 全文.
审查员 刘莹莹
权利要求书 6 页 说明书 21 页 附图 14 页

(54)发明名称

通信系统、装置和方法，信息处理设备和方法

(57)摘要

在预定覆盖区域内识别通信伙伴并以预定协议发送和接收信息的通信系统，包括装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该装置包括随机数产生单元、装置秘密密钥存储单元、通信ID发送单元和装置发送和接收单元。该信息处理设备包括设备加密单元、设备秘密密钥存储单元、通信ID存储单元、随机数获取单元和设备发送和接收单元。



CN 101162495 B

1. 一种在预定的覆盖区域内唯一地识别通信伙伴并以预定协议发送和接收信息的通信系统，该通信系统包括装置和信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，

该装置包括：

随机数产生部件，用于产生随机数；

装置加密部件，用于基于秘密密钥，根据预定的算法加密或者解密信息；

装置秘密密钥存储部件，用于存储秘密密钥，由用于加密和解密的装置加密部件使用该秘密密钥，并与信息处理设备预共享；

通信 ID 发送部件，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，且该通信 ID 是通过装置加密部件用秘密密钥根据随机数加密的 ID，该随机数是响应于从信息处理设备发送的轮询由随机数产生部件产生的；以及

装置发送和接收部件，用于向信息处理设备发送或者从其接收信息，该信息是使用由随机数产生部件产生的随机数作为密钥通过装置加密部件加密或者解密的；以及

该信息处理设备包括：

设备加密部件，基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储部件，用于存储秘密密钥，该秘密密钥被用于加密或者解密的设备加密部件使用，并与该装置预共享；

通信 ID 存储部件，用于存储包含在响应于轮询发送的然后从装置接收的响应中的通信 ID，该通信 ID 作为用于唯一地将该装置识别为通信伙伴的标识符；

随机数获取部件，通过设备加密部件用秘密密钥解密通信 ID 获得随机数；以及

设备发送和接收部件，用于向装置发送或者从其接收通过随机数获取部件用设备加密部件获得的随机数作为密钥加密或者解密的信息。

2. 一种在预定覆盖区内唯一地识别通信伙伴并以预定通信协议发送和接收信息的通信系统的通信方法，该通信系统包括装置和信息处理设备，其中在预定覆盖区内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该方法包括步骤：

响应于信息处理设备发送的轮询产生随机数；

向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定算法对所述响应于信息处理设备发送的轮询产生的随机数进行加密产生的；

向信息处理设备发送或者从其接收信息，该信息是用产生的随机数作为密钥根据算法加密或者解密的；

将包含在响应于轮询发送然后从该装置接收的响应中的通信 ID 存储为标识符，使用该标识符以唯一地将该装置识别为通信伙伴；

使用与该装置预共享的秘密密钥，根据预定算法，通过解密该通信 ID 获得随机数；以及

向该装置发送或者从其接收使用获得的随机数作为密钥根据算法加密或者解密的信息。

3. 一种在预定覆盖区域中唯一地识别通信伙伴并以预定的协议发送和接收信息的通

信系统中的装置，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该装置包括：

随机数产生部件，用于产生第一随机数；

装置加密部件，用于基于秘密密钥根据预定的算法加密或者解密信息；

装置秘密密钥存储部件，用于存储秘密密钥，该秘密密钥被用于加密和解密的装置加密部件使用，并与信息处理设备预共享；

通信 ID 发送部件，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密部件用秘密密钥根据第一随机数加密的 ID，该第一随机数是响应于从信息处理设备发送的轮询由随机数产生部件产生的；以及

装置发送和接收部件，用于向信息处理设备发送或者从其接收信息，该信息是使用由随机数产生部件产生的第一随机数作为密钥通过装置加密部件加密或者解密的。

4. 根据权利要求 3 的装置，其中该通信系统的通信协议包括近场通信接口和标准化为 ISO/IEC 18092 的协议 -1(NFCIP1)，以及

其中通信 ID 发送部件根据 NFCIP-1 将 NFC 标识符嵌入为通信 ID，在 RF 冲突避免和单一装置检测中使用该 NFC 标识符。

5. 根据权利要求 3 的装置，其中还包括 ID 存储部件，用于存储装置的唯一 ID，其中当从信息处理设备接收到读取唯一 ID 的请求时，该装置加密部件使用随机数产生部件产生的第一随机数作为密钥对存储在 ID 存储部件上的唯一 ID 加密，并将加密的唯一 ID 发送到信息处理设备。

6. 根据权利要求 5 的装置，还包括确定部件，用于确定唯一 ID 是否已经被加密然后将其发送到信息处理设备，

其中当确定部件确定唯一 ID 已经被加密并发送到信息处理设备时，装置发送和接收部件对将要与信息处理设备通信的信息加密或解密。

7. 根据权利要求 3 的装置，其中装置发送和接收部件使用随机数产生部件产生的第一随机数和用秘密密钥加密的、在轮询或者在轮询的下一次发送期间从信息处理设备发送的第二随机数，控制该装置加密部件对要与信息处理设备通信的信息加密和解密。

8. 一种在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的装置的通信方法，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该方法包括步骤：

响应于从信息处理设备发送的轮询产生随机数；

向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定算法通过对所述响应于从信息处理设备发送的轮询产生的随机数进行加密产生的；以及

发送或者接收信息，该信息是使用产生的随机数作为密钥根据算法加密或者解密的。

9. 一种在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的信息处理设备，该通信系统包括装置和该信息处理设备，其中在预定覆盖区域

内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该信息处理设备包括：

设备加密部件，基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储部件，用于存储秘密密钥，用于加密或者解密的设备加密部件使用该秘密密钥并与该装置预共享该秘密密钥；

通信 ID 存储部件，用于存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；

随机数获取部件，用于通过设备加密部件用秘密密钥解密通信 ID 获得第一随机数；以及

设备发送和接收部件，用于向装置发送或从其接收信息，该信息是用随机数获取部件获得的第一随机数通过设备加密部件加密或者解密的。

10. 根据权利要求 9 的信息处理设备，其中通信系统的通信协议包括近场通信接口和标准化为 ISO/IEC 18092 的协议 -1(NFCIP-1)，以及

其中通信 ID 存储部件将 NFC 标识符存储为通信 ID，该 NFC 标识符是响应于轮询在从该装置发送的响应中获得的，并在 NFCIP-1 中用于 RF 冲突避免和单一装置检测。

11. 根据权利要求 9 的信息处理设备，其中当读取该装置的唯一 ID 时，设备发送和接收部件加密或者解密将要与该装置通信的信息。

12. 根据权利要求 9 的信息处理设备，还包括用于产生第二随机数的随机数产生部件，

其中设备发送和接收部件用秘密密钥加密第二随机数并在轮询或者在轮询的下一次发送期间向该装置发送加密的第二随机数，并控制该设备加密部件以使用由随机数获取部件获得的第一随机数和第二随机数对要与该装置通信的信息加密或者解密。

13. 一种在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中信息处理设备的信息处理方法，该通信系统包括装置和该信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该信息处理方法包括步骤：

存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；

通过根据算法解密通信 ID 获取随机数，该算法是使用与该装置预共享的秘密密钥预定的；以及

向该装置发送和从其接收信息，该信息是使用获得的随机数作为密钥根据算法加密或者解密的。

14. 一种在预定覆盖区域内识别通信伙伴并以预定协议发送和接收信息的通信系统，该通信系统包括装置和信息处理设备，在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，

该装置包括：

装置随机数产生部件，用于产生第一随机数；

装置加密部件，用于基于秘密密钥根据预定的算法加密或者解密信息；

装置秘密密钥存储部件，用于存储秘密密钥，用于加密和解密的装置加密部件使用该秘密密钥，并与信息处理设备预共享该秘密密钥；

通信 ID 发送部件，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密部件用秘密密钥根据第一随机数加密的 ID，该第一随机数是通过响应于从信息处理设备发送的轮询由装置随机数产生部件产生的；以及

装置发送和接收部件，用于使用装置随机数产生部件产生的第一随机数和用秘密密钥加密的、在轮询或者轮询的下一次发送期间从信息处理设备发送的第二随机数，控制装置加密部件加密或者解密将要与信息处理设备通信的信息；以及

该信息处理设备包括：

设备随机数产生部件，用于产生第二随机数；

设备加密部件，用于基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储部件，用于存储秘密密钥，用于加密或者解密的设备加密部件使用该秘密密钥，并与该装置预共享该秘密密钥；

通信 ID 存储部件，存储包含在响应于轮询发送然后从该装置接收的响应中的通信 ID，该通信 ID 唯一地将该信息处理设备识别为通信伙伴；

随机数获取部件，用于通过设备加密部件用秘密密钥解密通信 ID 获得第一随机数；

设备发送和接收部件，用于用秘密密钥加密第二随机数，并在轮询或者在轮询的下一次发送期间向该装置发送加密的第二随机数，并空制该装置加密部件以使用由随机数获取部件获得的第一随机数和第二随机数对将要与该装置通信的信息加密或者解密。

15. 一种在预定覆盖区内唯一地识别通信伙伴并以预定通信协议发送和接收信息的通信系统的通信方法，该通信系统包括装置和信息处理设备，其中在预定覆盖区内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该方法包括步骤：

产生随机数；

向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定算法对响应于信息处理设备发送的轮询产生的第一随机数进行加密产生的；

向信息处理设备发送或者从其接收信息，该信息是根据算法使用产生的第一随机数和用该秘密密钥加密的、并在轮询或者轮询的下一次发送期间从信息处理设备发送的第二随机数作为密钥加密或者解密的；

产生第二随机数；

存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一将该装置识别为通信伙伴的标识符；

根据预定的算法通过用与该装置预共享的秘密密钥解密该通信 ID 获得第一随机数；以及

用该秘密密钥加密第二随机数，并在轮询或者在该轮询的下一次发送期间向该装置发送加密的秘密密钥，并发送或者接收使用获得的第一随机数和第二随机数根据算法加密或者解密的信息。

16. 一种在预定的覆盖区内唯一识别通信伙伴并以预定协议发送和接收信息的通信系统，该通信系统包括装置和信息处理设备，在预定覆盖区域内所述装置和信息处理设备中

的一个与所述装置和信息处理设备中的另一个进行无线通信，

该装置包括：

随机数产生单元，用于产生随机数；

装置加密单元，用于基于秘密密钥，根据预定的算法加密或者解密信息；

装置秘密密钥存储单元，用于存储秘密密钥，用于加密和解密的装置加密单元使用该秘密密钥，并与信息处理设备预共享该秘密密钥；

通信 ID 发送单元，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密单元用秘密密钥根据随机数加密的 ID，该随机数是响应于从信息处理设备发送的轮询由随机数产生单元产生的；以及

装置发送和接收单元，用于向信息处理设备发送或者从其接收信息，该信息是使用由随机数产生单元产生的随机数作为密钥通过装置加密单元加密或者解密的；以及

该信息处理设备包括：

设备加密单元，用于基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储单元，存储秘密密钥，该秘密密钥被用于加密或者解密的设备加密单元使用，并与该装置预共享；

通信 ID 存储单元，存储包含在响应于轮询发送的然后从装置接收的响应中的通信 ID，该通信 ID 是用于唯一地将该装置识别为通信伙伴的标识符；

随机数获取单元，通过设备加密单元用秘密密钥解密通信 ID 获得随机数；以及

设备发送和接收单元，用于向装置发送或者从其接收通过设备加密单元用随机数获取单元获得的随机数作为秘密密钥加密或者解密的信息。

17. 一种在预定覆盖区域中唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的装置，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该装置包括：

随机数产生单元，用于产生第一随机数；

装置加密单元，用于基于秘密密钥根据预定的算法加密或者解密信息；

装置秘密密钥存储单元，用于存储秘密密钥，该秘密密钥被用于加密和解密的装置加密单元使用，并与信息处理设备预共享；

通信 ID 发送单元，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别作为通信伙伴，并且该通信 ID 是通过装置加密单元用秘密密钥根据第一随机数加密的 ID，该第一随机数是响应于从信息处理设备发送的轮询由随机数产生单元产生的；和

装置发送和接收单元，用于向信息处理设备发送或者从其接收信息，该信息是使用由随机数产生单元产生的第一随机数作为密钥通过装置加密单元加密或者解密的。

18. 一种在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的信息处理设备，该通信系统包括装置和该信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，该信息处理设备包括：

设备加密单元，用于基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储单元，用于存储秘密密钥，用于加密或者解密的设备加密单元使用该秘密密钥，并与该装置预共享该秘密密钥；

通信 ID 存储单元，用于存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；

随机数获取元，通过设备加密单元用秘密密钥解密通信 ID 获得第一随机数；以及

设备发送和接收单元，用于向装置发送或从其接收信息，该信息是用随机数获取单元获得的第一随机数通过设备加密单元加密或者解密的。

19. 一种在预定覆盖区域内识别通信伙伴并以预定协议发送和接收信息的通信系统，该通信系统包括装置和信息处理设备，其中在预定覆盖区域内所述装置和信息处理设备中的一个与所述装置和信息处理设备中的另一个进行无线通信，

该装置包括：

装置随机数产生单元，用于产生第一随机数；

装置加密单元，用于基于预定的秘密密钥根据预定的算法加密或者解密信息；

装置秘密密钥存储单元，用于存储秘密密钥，用于加密和解密的装置加密单元使用该秘密密钥，并与信息处理设备预共享该秘密密钥；

通信 ID 发送单元，用于向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密单元用秘密密钥根据第一随机数加密的 ID，该第一随机数是通过响应于从信息处理设备发送的轮询由装置随机数产生单元产生的；以及

装置发送和接收单元，用于使用装置随机数产生单元产生的第一随机数和用秘密密钥加密的、并在轮询或者轮询的下一次发送期间从信息处理设备发送的第二随机数，控制装置加密单元加密或者解密将要与信息处理设备通信的信息；以及

该信息处理设备包括：

设备随机数产生单元，用于产生第二随机数；

设备加密单元，用于基于秘密密钥根据预定的算法加密或者解密信息；

设备秘密密钥存储单元，用于存储秘密密钥，用于加密或解密的设备加密单元使用该秘密密钥，并与该装置预共享该秘密密钥；

通信 ID 存储单元，用于存储包含在响应于轮询发送然后从该装置接收的响应中的通信 ID，该通信 ID 唯一地将该信息处理设备识别为通信伙伴；

随机数获取单元，通过设备加密单元用秘密密钥解密通信 ID 获得第一随机数；

设备发送和接收单元，用秘密密钥加密第二随机数并在轮询或者在轮询的下一次发送期间向该装置发送加密的第二随机数，并控制该装置加密单元以使用由随机数获取单元获得的第一随机数和第二随机数对要与该装置通信的信息加密或者解密。

通信系统、装置和方法，信息处理设备和方法

[0001] 相关申请的交叉引用

[0002] 本申请包含涉及2006年7月28日在日本专利局提交的日本专利申请JP2006-205702的主题，通过引用将其全部内容合并在此。

[0003] 技术领域

[0004] 本发明涉及一种用于通信的系统、装置和方法以及用于处理信息的设备和方法、计算机程序以及记录介质。更特别地，本发明涉及一种用于通信的系统、装置和方法，用于处理信息的设备以及方法、计算机程序记录介质，用于以简单布置(simple arrangement)进行安全和非常便利地通信。

[0005] 背景技术

[0006] 现在广泛使用不接触IC卡(contactless IC card)和射频识别(RFID)。如果多个不接触IC卡或者多个读/写器(reader/writer)在已知卡和读/写器之间的通信中发送无线波，那么每个卡或者每个读/写器就不能分别区分读/写器或者分别区分卡。这叫做RF冲突。为了避免RF冲突，单个卡使用只有其单个卡才有的唯一卡标识(ID)。

[0007] 当使用卡ID来避免冲突时，任何读/写器可以读取卡ID。可以容易地识别卡ID的持有者并可能侵犯持有者的隐私。

[0008] 可以给产品附加RFID，特别是当产品很少(rare)时展示其可靠性(authenticity)。附着到产品上的RFID是唯一的ID。用可以和RFID通信的任何读/写器，可以监控购买该产品的用户的活动。

[0009] 将在读/写器的通信覆盖区内识别IC卡和RFID的近场通信-接口和协议(NFCIP)标准化为ISO/IEC 18092(NFCIP-1)。根据这种标准，使用不发送到读/写器的ID卡或RFID的唯一ID避免了冲突。

[0010] 日本未审专利公开号2005-348306公开了一种保护隐私的方法。根据该公开内容，在每一个读/写器和RFID中的数字标记(tag)中建立秘密共享信息，并且只有具有秘密共享信息的读/写器可以解密经加密的信息。因此这些技术阻止了未被授权的跟踪，由此保护了隐私。

[0011] 发明内容

[0012] 然而，在NECIP-1中，没有将唯一ID发送到IC卡和RFID。不能识别IC卡和RFID。当每个IC卡和RFID需要被识别时，可以将IC卡或者RFID的唯一ID存储在每个芯片的数据区中，并根据需要发送到读/写器。在这种技术中，将唯一ID加密以保证安全发送，并需要交换会话秘密密钥的验证序列。

[0013] 在日本未审专利公开号2005-348306中公开的技术允许将数字标记的唯一ID保持为秘密的，但是只能应用到单向通信中。由于需要将识别信息在双向通信中进行的RFID中保持为是秘密的，所以不能识别通信伙伴。

[0014] 因此，理想的是以简单布置进行安全和方便的通信。

[0015] 根据本发明的一个实施例，一种通信系统，在预定的覆盖区内唯一识别通信伙伴并以预定协议发送和接收信息，包括：装置和信息处理设备，在预定覆盖区域内一个和另一

个进行无线通信。该装置包括用于产生随机数的随机数产生单元；用于基于预定的密钥根据预定的算法加密或者解密信息的装置加密单元；用于存储秘密密钥的装置秘密密钥存储单元，用于加密和解密的装置加密单元使用该秘密密钥并与信息处理设备预共享；用于向信息处理设备发送包含通信 ID 的响应的通信 ID 发送单元，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密单元用秘密密钥从随机数加密的 ID，该随机数是响应于从信息处理设备发送的轮询 (poll) 由随机数产生单元产生的；以及用于向信息处理设备发送或者从其接收信息的装置发送和接收单元，该信息是使用由随机数产生单元产生的随机数作为密钥通过装置加密单元加密或者解密的。信息处理设备包括用于基于预定密钥根据预定的算法加密或者解密信息的设备加密单元；用于存储秘密密钥的设备秘密密钥存储单元，该秘密密钥被用于加密或者解密的设备加密单元使用，并与该装置预共享；用于存储包含在响应于轮询发送的然后从装置接收的响应中的通信 ID 的通信 ID 存储单元，该通信 ID 作为用于唯一地将装置识别为通信伙伴的标识符；用设备加密单元的秘密密钥解密通信 ID 获得随机数的随机数获取单元；和用于向装置发送或者从其接收信息的设备发送和接收单元，该信息是通过设备加密单元用随机数获得单元获得的随机数作为密钥加密或者解密的。

[0016] 本发明的一个实施例涉及一种通信系统的通信方法，在预定覆盖区内唯一地识别通信伙伴并以预定通信协议发送和接收信息，该通信系统包括装置和信息处理设备，其中在预定覆盖区内一个和另一个进行无线通信。该方法包括步骤：产生随机 数；向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用由与信息处理设备预共享的秘密密钥根据预定算法对响应于从信息处理设备发送的轮询产生的随机数加密产生的；向信息处理设备发送或者从其接收信息，该信息是用产生的随机数作为密钥根据算法加密或者解密的；将包含在响应于轮询发送然后从该装置接收的响应中的通信 ID 存储为标识符，使用该标识符以唯一地识别装置作为通信伙伴；使用与该装置预共享的秘密密钥根据预定算法通过解密该通信 ID 获得随机数；并向该装置发送或者从其接收信息，该信息是使用获得的随机数作为密钥，根据算法加密或者解密的。

[0017] 根据本发明的实施例，该装置产生随机数；向信息处理装置发送包含通信 ID 的响应；该通信 ID 唯一地将信息处理设备识别为通信伙伴，其是用与信息处理设备预共享 (pre-share) 的秘密密钥根据预定算法对响应于从信息处理设备发送来的轮询所产生的随机数加密产生的；向信息处理设备发送或者从其接收信息，该信息是用产生的随机数作为密钥根据算法加密或者解密的。该信息处理设备将包含在响应于轮询发送并然后从该装置接收的响应中的通信 ID 作为标识符存储，使用该标识符以唯一地将装置识别为通信伙伴；通过使用与该装置预共享的秘密密钥根据预定算法解密通信 ID 获得随机数；并向该装置发送或者从其接信息，该信息是使用获得的随机数作为密钥，根据算法加密或者解密的。

[0018] 本发明的一个实施例涉及在预定覆盖区域中唯一地识别通信伙伴并以预定的协议发送和接收信息通信系统中的装置，该通信系统包括装置和信息处理设备，其中在预定覆盖区域内一个与另一个进行无线通信。该装置包括用于产生第一随机数的随机数产生单元；基于预定的密钥根据预定的算法加密或者解密信息的装置加密单元；用于存储秘密密钥的装置秘密密钥存储单元，该秘密密钥被用于加密和解密的装置加密单元使用并与信息处理设备预共享；用于向信息处理设备发送包含通信 ID 的响应的通信 ID 发送单元，该通信

ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是由装置加密单元用秘密密钥从第一随机数加密的 ID，该第一随机数是响应于从信息处理设备发送的轮询由随机数产生单元产生的；以及用于向信息处理设备发送或者从其接收信息的装置发送和接收单元，该信息是使用由随机数产生单元产生的第一随机数作为密钥通过装置加密单元加密或者解密的。

[0019] 通信系统的通信协议包括近场通信接口和被标准化为 ISO/IEC18092 的协议 -1(NFCIP-1)。根据 NFCIP-1，通信 ID 发送单元可以嵌入 NFC 标识符作为通信 ID，该 NFC 标识符用于 RF 冲突避免和单一装置检测中。

[0020] 该装置还可以包括用于存储装置的唯一 ID 的 ID 存储单元。当从信息处理设备接收到读取唯一 ID 的请求时，该装置加密单元使用随机数产生单元产生的第一随机数作为密钥对存储在 ID 存储单元上的唯一 ID 加密，并将加密的唯一 ID 发送到信息处理设备。

[0021] 该装置还可以包括确定唯一 ID 是否已经被加密然后发送到信息处理设备的确定单元。当确定单元确定唯一 ID 已经被加密并发送到信息处理设备时，装置发送和接收单元对要与信息处理设备通信的信息加密或者解密。

[0022] 装置发送和接收单元使用随机数产生单元产生的第一随机数和并在轮询期间或者在轮询的下一发送期间从信息处理设备发送的、用秘密密钥加密的第二随机数控制该装置加密单元对要与信息处理设备通信的信息进行加密和解密。

[0023] 本发明一个实施例涉及一种在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的装置的通信方法，，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该方法包括步骤：产生随机数；向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且是通过用与信息处理设备预共享的秘密密钥根据预定算法对响应于从信息处理设备发送的轮询产生的随机数加密产生的，并发送或者接收信息，该信息是使用产生的随机数作为密钥根据算法加密或者解密的。

[0024] 本发明的一个实施例涉及一种使得在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的装置执行该装置的通信方法的计算机可读程序，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该计算机程序包括步骤：产生随机数；向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过用与信息处理设备预共享的秘密密钥根据预定算法对响应于从信息处理设备发送的轮询产生的随机数加密产生的；以及发送或者接收信息，该信息是使用产生的随机数作为密钥根据算法加密或者解密的。

[0025] 根据本发明的实施例，产生随机数。将包含通信 ID 的响应发送到信息处理设备。通信 ID 唯一地将信息处理设备识别为通信伙伴，并且是根据用与信息处理设备预共享的秘密密钥根据预定算法通过对响应于从信息处理设备发送的轮询产生的随机数加密产生的，以及发送或者接收信息，该信息是使用产生的随机数作为密钥根据算法加密或者解密的。

[0026] 本发明的一个实施例涉及在预定覆盖区域内唯一地识别通信伙伴并以预定的 协议发送和接收信息的通信系统中的一种信息处理设备，该通信系统包括该装置和信息处理

设备，其中在预定覆盖区域内一个和另一个进行无线通信。该信息处理设备包括用于基于预定的密钥根据预定的算法加密或者解密信息的设备加密单元；用于存储秘密密钥的设备秘密密钥存储单元，用于加密或者解密的设备加密单元使用该秘密密钥并与该装置预共享该秘密密钥；通信 ID 存储单元，用于存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID，该通信 ID 作为用于唯一地将该装置识别为通信伙伴的标识符；随机数获取单元，通过由设备加密单元用秘密密钥解密通信 ID 来获得第一随机数；以及设备发送和接收单元，用于向装置发送或从其接收信息，该信息是通过设备加密单元用随机数获取单元获得的第一随机数加密或者解密的。通信系统的通信协议可以包括近场通信接口和标准化为 ISO/IEC18092 的协议 -1(NFCIP-1)。通信 ID 存储单元存储 NFC 标识符以作为通信 ID，该 NFC 标识符是响应于轮询在从该装置发送的响应中获得的，并在 NFCIP-1 中用于 RF 冲突避免和单一装置检测。

[0027] 信息处理设备还可以包括用于产生第二随机数的随机数产生单元。设备发送和接收单元用秘密密钥对第二随机数加密并在轮询或者该轮询的下一次发送期间将加密的第二随机数发送到该装置，并使用由随机数获取单元获得的第一随机数和第二随机数控制设备加密单元对与该装置通信的信息加密或者解密。

[0028] 当读取装置的唯一 ID 时，设备发送和接收单元可以加密或者解密要与该装置通信的信息。

[0029] 本发明的一个实施例涉及在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统中的信息处理设备的信息处理方法，该通信系统包括该装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该信息处理方法包括步骤：存储包含在响应于轮询发送然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；通过根据算法解密通信 ID 获得随机数，该算法是使用与该装置预共享的秘密密钥预定的，并向该装置发送或者从其接收信息，该信息是使用获得的随机数作为密钥根据算法加密或者解密的。

[0030] 本发明的一个实施例涉及一种计算机可读程序，使得信息处理设备执行在预定覆盖区域内唯一地识别通信伙伴并以预定的协议发送和接收信息的通信系统的通信处理方法，该通信系统包括装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该计算机可读程序包括步骤：存储包含在响应于轮询发送然后 从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；通过根据算法解密通信 ID 获得随机数，该算法是使用与该装置预共享的秘密密钥预定的，并且向该装置发送或者从其接收信息，该信息是使用获得的随机数作为密钥根据该算法加密或解密的。

[0031] 存储包含在响应于轮询发送的然后从该装置接收的响应中的通信 ID。该通信 ID 是唯一地将该装置识别为通信伙伴的标识符。通过根据算法解密通信 ID 获得随机数，该算法是使用与该装置预共享的秘密密钥预定的。发送或者接收使用获得的随机数根据算法加密或者解密的信息。

[0032] 本发明的一个实施例涉及一种在预定覆盖区域内唯一地识别通信伙伴并以预定协议发送和接收信息的通信系统。通信系统包括装置和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该装置包括用于产生第一随机数的装置随机数产生单元；用于基于预定的秘密密钥根据预定的算法加密或者解密信息的装置加密单元；用于存

储秘密密钥的装置秘密密钥存储单元，用于加密和解密的装置加密单元使用该秘密密钥并与信息处理设备预共享该秘密密钥；向信息处理设备发送包含通信 ID 的响应的通信 ID 发送单元，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是通过装置加密单元用秘密密钥从第一随机数加密的 ID，该第一随机数是通过响应于从信息处理设备发送的轮询由装置随机数产生单元产生的；以及装置发送和接收单元，用于在轮询或者轮询的下一次发送期间，使用随机数产生单元产生的第一随机数和用秘密密钥加密的并从信息处理设备发送的第二随机数，控制装置加密单元加密或者解密将与信息处理设备通信的信息。信息处理设备包括用于产生第二随机数的设备随机数产生单元；用于基于预定密钥根据预定的算法加密或者解密信息的设备加密单元；用于存储秘密密钥的设备秘密密钥存储单元，用于加密或者解密的设备加密单元使用该秘密密钥并与该装置预共享该秘密密钥；用于存储包含在响应于轮询发送然后从该装置接收的响应中的通信 ID 的通信 ID 存储单元，该通信 ID 唯一地将该信息处理设备识别为通信伙伴；是由装置加密单元用秘密密钥解密通信 ID 获得第一随机数的随机数获取单元；以及设备发送和接收单元，用于用秘密密钥加密第二随机数，并在轮询时或轮询的第二次发送时将加密的第二随机数发送到该装置，并控制装置加密单元使用由随机数获取单元获得的第一随机数和第二随机数加密或者解密将要与该装置通信的信息。

[0033] 本发明的一个实施例涉及在预定覆盖区域内唯一地识别通信伙伴并以预定协议发送和接收信息的通信系统的通信方法，该通信系统包括装置和信息处理设备， 其中在预定覆盖区域内一个和另一个进行无线通信。该通信方法包括步骤：产生第一随机数；将包含通信 ID 的响应发送到信息处理设备；该通信 ID 唯一地将该信息处理设备识别为通信伙伴，且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定的算法对第一随机数加密所产生的，该第一随机数是响应于从信息处理设备发送的轮询产生的；向信息处理设备发送或者从其接收信息，该信息是使用生成的第一随机数和用秘密密钥加密的、在轮询期间或轮询之后的下一个发送期间从信息处理设备发送的第二随机数作为密钥根据算法加密或解密的；产生第二随机数，存储包含在响应中的通信 ID，该响应是响应于轮询发送然后从该装置接收的，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符；根据预定算法通过用与该装置预共享的秘密密钥对通信 ID 解密获得第一随机数，并在轮询或者该轮询的下一次发送期间用秘密密钥加密第二随机数并向该装置传送加密的秘密密钥；以及发送或者接收信息，该信息是使用获得的第一随机数和第二随机数根据算法被加密或者解密的。

[0034] 根据本发明的实施例，该装置产生第一随机数，向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定的算法，对响应于从信息处理设备发送的轮询产生的第一随机数进行加密产生的，并向信息处理设备发送或者从其接收信息，该信息是使用产生的第一随机数和用秘密密钥加密的、在轮询或者在该轮询的下一次发送期间从信息处理设备发送的第二随机数作为密钥，根据算法加密或者解密的。该信息处理设备产生第二随机数；存储包含在响应中的通信的 ID，该响应是响应于轮询发送然后从该装置接收的，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符，通过根据预定算法用与该装置预共享的秘密密钥对通信 ID 解密获得第一随机数，并在轮询或者该轮询的下一次发送期间，用秘密密钥

对第二随机数加密并向该装置传送加密的秘密密钥，以及发送或者接收信息，该信息是使用获得的第一随机数和第二随机数根据算法被加密或者解密的。

[0035] 根据本发明的实施例，可以以简单的布置进行安全和便利的通信。

附图说明

[0036] 图 1 是示出了根据本发明的一个实施例的通信系统的方框图；

[0037] 图 2 是示出了具有图 1 的 IC 卡的通信处理的流程图；

[0038] 图 3 示出了由 NFCIP-1 定义的响应形式格式 (response form format)；

[0039] 图 4 是示出了在图 1 所示的读 / 写器和 IC 卡之间进行的通信的流程图；

[0040] 图 5 示出了通信 ID 产生处理的流程图；

[0041] 图 6 是示出了随机数获取处理的流程图；

[0042] 图 7 是示出了卡 ID 发送处理的流程图；

[0043] 图 8 是示出了卡 ID 解密处理的流程图；

[0044] 图 9 是示出了读取数据发送处理的流程图；

[0045] 图 10 是示出了写请求发送处理的流程图；

[0046] 图 11 是示出了写数据处理的流程图；

[0047] 图 12 是详细示出了在本发明的一个实施例的 IC 卡和已知读 / 写器之间进行的通信的流程图；

[0048] 图 13 是示出了根据本发明的另一个实施例的通信系统的方框图；

[0049] 图 14 是具体示出了在图 13 的读 / 写器和 IC 卡之间进行的通信的流程图；

[0050] 图 15 是示出了轮询请求产生处理的流程图；

[0051] 图 16 是示出了随机数 B 获取处理的流程图；

[0052] 图 17 是具体示出了图 13 的读 / 写器和 IC 卡之间进行的通信的流程图；

[0053] 图 18 是示出了卡 ID 读取请求产生处理的流程图；以及

[0054] 图 19 是示出了随机数 B 获取处理的流程图。

具体实施方式

[0055] 在描述本发明的实施例之前，下面讨论本发明的特征和在本发明的说明书或者附图中公开的实施例之间的对应关系。这种陈述的目的是保证在该说明书或者附图中描述支持所要求的发明的实施例。因此，即使在说明书或者附图中描述实施例，而不是在这里描述成关于本发明的特征，也不必然意味着该实施例不涉及本发明的特征。相反，即使在这里实施例描述成关于本发明的特定特征，但是也不必然意味着该实施例不涉及本发明的其它特征。

[0056] 根据本发明的一个实施例，在预定覆盖区域内唯一地识别通信伙伴并以预定协议发送和接收信息的通信系统，包括在预定覆盖区域内一个和另一个进行无线通信的装置（例如，图 1 的 IC 卡 200）和信息处理设备（例如图 1 的读 / 写器 100）。该装置包括用于产生随机数的随机数产生单元（例如，图 1 的随机数产生器 202）；用于基于预定密钥根据预定算法加密或者解密信息的装置加密单元（例如，图 1 的加密处理器 208）；用于存储秘密密钥的装置秘密密钥存储单元（例如，图 1 的秘密密钥存储单元 203），其中由用于加密和

解密的装置加密单元使用秘密密钥并与信息处理 设备预共享；用于向信息处理设备发送包含通信 ID 的响应的通信 ID 发送单元（例如，图 1 的执行图 4 的步骤 S103 的 CPU207），其中该通信 ID 唯一地将信息处理设备识别为通信伙伴通信，并且该通信 ID 是通过装置加密单元用秘密密钥从随机数加密的 ID，该随机数是响应于从信息处理设备发送的轮询而由随机数产生单元产生的；以及用于向信息处理设备发送或者从其接收信息的装置发送和接收单元（例如，执行图 4 的步骤 S108 和 S110 中的一个步骤的图 1 的 CPU207），该信息是使用由随机数产生单元产生的随机数作为密钥通过装置加密单元加密或者解密的信息。该信息处理设备包括用于基于预定的密钥根据预定的算法加密或者解密信息的设备加密单元（例如，图 1 的加密处理器 208）；用于存储秘密密钥的设备秘密密钥存储单元（例如图 1 的秘密密钥存储单元 203），用于加密或者解密的设备加密单元使用该秘密密钥并与装置预共享；用于存储包含在响应于轮询而发送并从该装置接收的响应中的通信 ID 的通信 ID 存储单元（例如，执行图 6 的步骤 S332 的图 1 的 CPU105），该通信 ID 是用于唯一地将该装置识别为通信伙伴的标识符；用于通过装置加密单元用秘密密钥解密通信 ID 获取随机数的随机数获取单元（例如，执行图 6 的步骤 S334 的图 1 的 CPU105）；和用于向装置发送或者从其接收信息的设备发送和接收单元（例如，执行图 4 的步骤 S206、S209 和 S210 中的一个步骤的图 1 的 CPU105），该信息是通过随机数获取单元用装置加密单元获得的随机数作为密钥进行加密或者解密的。

[0057] 本发明的一个实施例涉及一种在预定覆盖区域内唯一地标识通信伙伴并以预定通信协议发送和接收信息的通信系统的通信方法，该通信系统包括装置（例如，图 1 的 IC 卡 200）和信息处理设备（例如，图 1 的读 / 写器 100），其中在预定覆盖区域内一个和另一个进行无线通信。该方法包括步骤：产生随机数（例如，在图 5 的步骤 S301 中）；向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定算法对响应于从信息处理设备发送的轮询而产生的随机数进行加密产生的（例如，在图 4 的步骤 S103 中）；向信息处理设备发送或者从其接收信息，该信息是用产生的随机数作为密钥根据算法加密或者解密的（例如在图 4 的步骤 S108 和 S110 的其中一个步骤中）；将包含在响应于轮询而发送然后从该装置接收的响应中的通信 ID 作为标识符存储，使用该标识符以唯一地将装置标识为通信伙伴（例如，在图 6 的步骤 S332 中）；使用与该装置预共享的秘密密钥根据预定算法通过解密通信 ID 获得随机数（例如，在图 6 的步骤 S334 中）；并向该装置发送或者从其接收信息，该 信息是使用作为密钥的所获得的随机数，根据算法加密或者解密的（例如，图 4 的步骤 S206、S209 和 S210 的其中一个步骤）。

[0058] 本发明的一个实施例涉及在预定覆盖区域中唯一地标识通信伙伴并以预定的协议发送和接收信息的通信系统中的装置（例如，图 1 的 IC 卡 200），该通信系统包括装置和信息处理设备（例如，图 1 的读 / 写器 100），其中在预定覆盖区域内一个与另一个进行无线通信。该装置包括用于产生第一随机数的随机数产生单元（例如，图 1 的随机数产生器 202）；用于基于预定密钥根据预定的算法加密或者解密信息的装置加密单元（例如，图 1 的加密处理器 208）；用于存储秘密密钥的装置秘密密钥存储单元（例如，图 1 的秘密密钥存储单元 203），该秘密密钥被用于加密和解密的装置加密单元使用并与信息处理设备预共享；用于向信息处理设备发送包含通信 ID 的响应的通信 ID 发送单元（例如，执行图 4 的步

骤 S103 的图 1 的 CPU207)，该通信 ID 唯一地将信息处理设备识别为通信伙伴，且该通信 ID 是通过装置加密单元用秘密密钥从第一随机数加密的 ID，该第一随机数是响应于从信息处理设备发送的轮询由随机数产生单元产生的；以及用于向信息处理设备发送或者从其接收信息的装置发送和接收单元（例如，执行图 4 的步骤 S108 和 S110 中的一个步骤的图 1 的 CPU207)，该信息是使用由随机数产生单元产生的随机数作为密钥通过装置加密单元加密或者解密的。

[0059] 通信系统的通信协议可以包括近场通信接口和标准化为 ISO/IEC18092 的协议 -1(NFCIP-1)。根据 NFCIP-1，通信 ID 发送单元可以嵌入为通信 ID 和 NFC 标识符（例如，图 3 的 NFCID2)，在 RF 冲突避免和单一装置检测中使用该 NFC 标识符。

[0060] 该装置还可以包括用于存储装置的唯一 ID 的 ID 存储单元（例如，图 1 的 ID 存储单元 204)。当从信息处理设备接收到读取该唯一 ID 的请求时，该装置加密单元使用由随机数产生单元产生的第一随机数作为密钥对存储在 ID 存储单元中的唯一 ID 加密，并将加密的唯一 ID 发送到信息处理设备。

[0061] 该装置还可以包括用于确定确定唯一 ID 是否已经被加密然后将其发送到信息处理设备的确定单元（例如执行图 2 的步骤 S29 的图 1 的 CPU207)。当确定单元确定唯一 ID 已经被加密并发送到信息处理设备时，装置发送和接收单元对要与信息处理设备通信的信息加密或解密。

[0062] 本发明的一个实施例涉及在预定覆盖区域中唯一地标识通信伙伴并以预定的协议发送和接收信息的通信系统中的装置（例如，图 1 的 IC 卡 200) 的通信方法，该通信系统包括装置和信息处理设备（例如，图 1 的读 / 写器 100)，其中在预定覆盖 区域内一个与另一个进行无线通信。该方法包括步骤：产生随机数（例如，在图 5 的步骤 S301 中）；向信息处理设备发送包含通信 ID 的响应，该通信 ID 唯一地将信息处理设备识别为通信伙伴，并且该通信 ID 是用与信息处理设备预共享的秘密密钥根据预定算法加密通过响应于从信息处理设备发送的轮询产生的随机数而产生的（例如，在图 1 的步骤 S103 中）；以及发送或者接收信息，该信息是使用产生的随机数作为密钥根据算法加密或者解密的（例如，在图 4 的步骤 S108 和 S110 的其中一个步骤中）。

[0063] 本发明的一个实施例涉及在预定覆盖区域内唯一地标识通信伙伴并以预定的协议发送和接收信息的通信系统中的一种信息处理设备（例如，图 1 的读 / 写器 100)，该通信系统包括装置（例如，图 1 的 IC 卡 200) 和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该信息处理设备包括用于基于预定的密钥根据预定的算法加密或者解密信息的设备加密单元（例如，图 1 的加密处理器 208)；用于存储秘密密钥的设备秘密密钥存储单元（例如，图 1 的秘密密钥存储单元 203)，由用于加密或者解密的设备加密单元使用该秘密密钥并与该装置预共享秘密密钥；用于存储包含在响应于轮询而发送然后从该装置接收的响应中的通信 ID 的通信 ID 存储单元（例如，执行图 6 的步骤 S332 的图 1 的 CPU105)，该通信 ID 为用于唯一地将该装置标识为通信伙伴的标识符；用于通过设备加密单元用秘密密钥对通信 ID 解密获得第一随机数的随机数获取单元（例如，执行图 6 的步骤 S334 的图 1 的 CPU105)；和用于向装置发送或从其接收信息的设备发送和接收单元（例如，用于执行图 4 的步骤 S206、S209 和 S210 的其中一个步骤的图 1 的 CPU105)，该信息是由设备加密单元用随机数获取单元获得的第一随机数加密或者解密的。

[0064] 通信系统的通信协议可以包括近场通信接口和标准化为 ISO/IEC18092 的协议 -1(NFCIP-1)。通信 ID 存储单元存储作为通信 ID 的 NFC 标识符（例如，图 3 的 NFCID2），该 NFC 标识符是响应于轮询在从该装置发送的响应中获得的，并在 RF 冲突避免和 NFCIP-1 中的单一装置检测中使用。

[0065] 本发明的一个实施例涉及在预定覆盖区域内唯一地标识通信伙伴并以预定的协议发送和接收信息的通信系统中信息处理装置（例如，图 1 的读 / 写器 100）的信息处理方法，该通信系统包括装置（例如，图 1 的 IC 卡 200）和信息处理设备，其中在预定覆盖区域内一个和另一个进行无线通信。该信息处理方法包括步骤 :存储包含在响应于轮询而发送然后从该装置接收的响应中的通信 ID，该通信 ID 是唯一地将该装置识别为通信伙伴的标识符（例如，在图 6 的步骤 S332 中）;通过根据算 法解密通信 ID 获得随机数，该算法是使用与该装置预共享的秘密密钥预定的（例如在图 6 的步骤 S334 中），并向该装置发送或者从其接收信息，该信息是使用获得的随机数作为密钥根据算法加密或者解密的（例如，在图 4 的步骤 S206、S209 和 S210 的其中一个步骤中）。

[0066] 下面参考附图描述本发明的实施例。

[0067] 图 1 是示出了根据本发明的一个实施例的通信系统 50 的方框图。如图 1 所示，通信系统 50 包括读 / 写器 100 和 IC 卡 200。读 / 写器 100 和 IC 卡 200 使用其天线以无线方式彼此通信。

[0068] 读 / 写器 100 中的输入输出单元 102 发送预定的无线电波并当发送无线电波时检测其天线上的负载的变化。当 IC 卡 200 向其靠近时输入输出单元 102 由此检测 IC 卡 200。读 / 写器 100 具有天线，当 IC 卡 200 接近读 / 写器 100 时天线向 IC 卡 200 发送和从其接收多种数据。输入输出单元 102 根据从 CPU105 提供的数据以从振荡 (OSC) 电路提供的预定频率幅移键控 (ASK) 调制载波，并从天线输出调制波作为无线电波。输入输出单元 102 还解调通过天线接收到的 ASK 调制波，并向 CPU105 提供解调的数据。

[0069] 读 / 写器 100 中的中央处理单元 (CPU)105 将存储在只读存储器 (ROM)104 上的程序装载到随机存取存储器 (RAM)103，由此执行各种处理。RAM103 存储 CPU105 执行各种处理需要的数据。

[0070] CPU105 控制加密处理器 106，由此根据预定的加密算法加密或者解密数据。加密处理器 106 的加密算法是秘密密钥密码系统中的一种，例如数据加密标准 (DES)、三倍的 DES，或者高级加密标准 (AES)。

[0071] 当读 / 写器 100 加密或者解密数据时，CPU105 向加密处理器 106 一起提供存储在秘密密钥存储单元 101 上的秘密密钥和被加密或者解密的数据。加密处理器 106 由此使用提供的秘密密钥加密或者解密所提供的数据。

[0072] 存储在秘密密钥存储单元 101 上的秘密密钥与存储在 IC 卡 200 中的秘密密钥存储单元 203 上的秘密密钥相同。秘密密钥仅仅预存储在对应于 IC 卡 200 的读 / 写器 100 上并允许该读 / 写器 100 读取对于 IC 卡 200 唯一的卡标识 (ID)。

[0073] IC 卡 200 中的输入输出单元 201 包括由线圈天线 (coiled antenna) 和电容器构成的电感器电容器 (LC) 电路。将输入输出单元 201 中的 LC 电路设计成与从放置在附近的读 / 写器 100 发送的预定频率的无线电波发生谐振。输入输出单元 201ASK 解调响应于天线中激励的交变电磁场产生的电信号，借此对电信号进行整流。输入 输出单元 201 调整整

流的电信号，并向 IC 卡 200 中的每个部分提供调整的电信号作为直流电源。调节从读 / 写器 100 发送的无线电波的功率来产生足够向 IC 卡 200 供电的电磁场。

[0074] 输入输出单元 201 由此包络检测通过天线接收的 ASK 调制波，二元相移键控 (BPSK) 解调 ASK 解调的信号，并向 CPU207 提供 BPSK 解调的信号。输入输出单元 201 产生具有与接收到的信号的时钟信号相同频率的时钟信号，并向 CPU207 提供产生的时钟信号。

[0075] 为了向读 / 写器 100 发送预定的信息，输入输出单元 201 响应于天线的负载中的变化 ASK 调制由 CPU207 提供的 BPSK 调制数据，然后通过天线向读 / 写器 100 发送调制的分量。

[0076] IC 卡 200 中的输入输出单元 201 执行存储在 ROM206 上的多个程序。秘密密钥存储单元 203、ID 存储单元 204 和数据存储单元 205 被布置在电可擦除可编程只读存储器 (EEPROM) 中的各个部分中。

[0077] CPU207 通过控制加密处理器 208 用预定的加密算法加密或者解密数据。加密处理器 208 的加密算法是秘密密钥密码系统中的一种，并与加密处理器 106 的加密算法相同。

[0078] 当 IC 卡 200 加密或者解密数据时，CPU207 向加密处理器 208 一起提供存储在秘密密钥存储单元 203 上的秘密密钥和被加密或者解密的数据。加密处理器 208 由此根据提供的秘密密钥对提供的数据进行加密或者解密。

[0079] 随机数产生器 202 根据需要产生预定位数的随机数。如后面将要描述的，在 IC 卡 200 和读 / 写器 100 之间的通信中使用随机数，作为互相识别通信伙伴的会话 ID 和用于加密或者解密会话中通信的数据的会话秘密密钥。

[0080] ID 存储单元 204 存储卡 ID 作为 IC 卡 200 唯一标识信息。

[0081] 根据需要，数据存储单元 205 存储应用数据，用于提供 IC 卡 200 的多种服务。

[0082] 可以使用软件实施加密处理器 106 和加密处理器 208 中的每一个。

[0083] 由于读 / 写器 100 和 IC 卡 200 执行无线通信，所以可能发生冲突。在冲突中，IC 卡或者读 / 写器中的每一个都不能识别是读 / 写器或者 IC 卡中的哪一个发送无线电波。然而，在通信系统 50 中，读 / 写器 100 和 IC 卡 200 中的每一个执行按照近场通信 - 接口和协议 (NFCIP) 的通信，该近场通信 - 接口和协议可以识别置于读 / 写器的通信覆盖范围内的 IC 卡或者 RFID。

[0084] NFCIP-1 标准合并了 RF 检测和冲突避免机制以允许 NFCIP-1 装置以另一个装 置也能工作的频带进行通信。在 NFCIP-1 标准中使用 NFCID(NFC 标识符) 和 NFC 装置标识符。NFCIP 是使用用于冲突避免和单一装置检测处理的随机数的 NFC 装置标识符。在已知的典型通信系统中，将 IC 卡唯一的 ID 发送到读 / 写器，读 / 写器基于该用于冲突避免的 ID 识别 IC 卡。NFCIP-1 标准不需要 IC 卡的唯一 ID 发送到读 / 写器。

[0085] 在通信系统 50 中，读 / 写器 100 和 IC 卡 200 中的每一个都识别通信伙伴以防止冲突，而不需要 IC 卡 200 向读 / 写器 100 发送唯一卡 ID。

[0086] 在 ISO/IEC18092 规范中详细描述了 NFCIP-1 标准。

[0087] 在下述的讨论中，读 / 写器 100 起到在 NFCIP-1 标准中定义的启动器 (initiator) 的作用并且 IC 卡 200 起到 NFCIP-1 标准中定义的目标的作用。在 NFCIP-1 标准的无源通信模式中，启动器和目标的每一个都按照 106kb/s 的数据传输率或者 212kb/s 和 424kb/s 中的一个数据传输率。现在假设启动器和目标中的每一个都以 212kb/s 和 424kb/s 中的一

个数据传输率工作。

[0088] 如上所述，通信系统 50 进行无线通信而没有从 IC 卡 200 发送唯一卡 ID 到读 / 写器 100。通信系统 50 由此提供隐私保护。然而，使用 IC 卡的服务仍然需要唯一地识别单个 IC 卡的机构。根据本发明的一个实施例，IC 卡 200 仍然合并有向读 / 写器 100 发送对于 IC 卡 200 唯一的卡 ID 的机构。

[0089] 图 2 示出了图 1 的 IC 卡 200 的通信处理的流程图。例如当将输入输出单元 201 的天线中激励的 AC 磁场产生的电力馈送给置于靠近读 / 写器 100 的天线处的 IC 卡 200 的每一个部分时，启动通信处理。

[0090] 在步骤 S21，随机数产生器 202 产生随机数。将这里产生的随机数存储在数据存储单元 205 上的预定区域中。

[0091] 在步骤 S22，加密处理器 208 用存储在秘密密钥存储单元 203 上的秘密密钥对在步骤 S21 中产生的随机数加密，以产生通信 ID。

[0092] 在步骤 S23，CPU207 确定是否已经从读 / 写器 100 接收到轮询请求。CPU207 在备用状态上等待，直到已经从读 / 写器 100 接收到轮询请求。如果在步骤 S23 确定中确定已经接收到轮询请求，则处理进行到步骤 S24。

[0093] 在步骤 S24，CPU207 向读 / 写器 100 发送答复在步骤 S23 中确定接收到的轮询请求的轮询响应。该响应包含在步骤 S22 中产生的通信 ID。

[0094] 图 3 示出了响应帧的格式，以 NFCIP-1 标准定义该格式并且存储发送的响应的数据。当启动器和目标中的每一个都运行在 212kb/s 和 424kb/s 中的一个数据传输率 时，响应来自启动器的轮询请求从目标发送响应帧。

[0095] 所示的“前同步码 (preamble)”字段存储至少其中的 48 位都是逻辑“0”的数据。“同步模式 (synchronization pattern)”存储用于在启动器和目标之间通信同步的 2 字节 (16 位) 数据。“长度 (length)”字段存储表示值为“12”的 8 位数据。“有效负载 (payload)”字段存储由起始字节“01”、8 字节 NFCID2 和 8 字节填充 (Pad) 构成的数据。“循环冗余校验 (cyclic redundancy check，CRC)”字段存储用于错误检验的数据，其是以预定方法计算的。

[0096] 在步骤 S24，将通信 ID 存储为有效负载字段中的 NFCID2。由此发送响应帧。

[0097] 如上所述，通信 ID 是加密的随机数。对应于 IC 卡 200 并允许读取 IC 卡 200 的卡 ID 的读 / 写器 100 在秘密密钥存储单元 101 上存储秘密密钥，该秘密密钥与存储在秘密密钥存储单元 203 上的秘密密钥相同。读 / 写器 100 解密步骤 S24 中传送的响应帧的 NFCID2(通信 ID) 值，从而获取步骤 S21 中 IC 卡 200 产生的随机数。

[0098] 回到图 2，CPU207 在步骤 S24 之后的步骤 S25 确定是否已经从读 / 写器 100 接收到指令，CPU207 在备用状态上等待，直到确定出已经从读 / 写器 100 接收到指令。读 / 写器 100 向 IC 卡 200 发送预定的指令。以读取存储在 IC 卡 200 上的数据或者在 IC 卡 200 上写入数据。如果在步骤 S25 确定出已经从读 / 写器 100 接收到指令，则处理进行到步骤 S26。

[0099] 在步骤 S26，CPU207 确定在步骤 S25 接收到的指令是否是请求发送 IC 卡 200 的唯一卡 ID 的指令。如果在步骤 S26 中确定指令是请求发送卡 ID 的指令，则处理进行到步骤 S27。

[0100] 在步骤 S27，CPU207 将加密标记设置为 ON。由此加密要在随后的处理中发送的数据。加密标记是数据存储单元 205 中的预定区域中的一位。加密标记的缺省设置是“0(OFF)”。一旦将加密标记设置为 ON，则加密标记保持为 ON 直到停止向 IC 卡 200 提供电源，也就是直到 IC 卡 200 移出读 / 写器 100 的通信覆盖区域。

[0101] 在步骤 S28，CPU207 读取存储在 ID 存储单元 204 上的卡 ID，控制加密处理器 208 以用在步骤 S21 中产生的随机数作为密钥来加密卡 ID，并向读 / 写器 100 发送加密的卡 ID。以这种方式，当已经从读 / 写器 100 接收到请求发送卡 ID 的发送请求时，IC 卡 200 用随机数作为密钥来加密卡 ID 并向读 / 写器 100 发送加密的卡 ID。

[0102] 用如上所述获取的随机数，读 / 写器 100 可以解密在步骤 S28 中发送的数据，由此获取卡 ID。

[0103] 在步骤 S28 之后处理回到步骤 S25 执行步骤 S25 和 S26。如果在步骤 S26 确定 指令不是请求发送卡 ID 的指令，则处理进行到步骤 S29。从读 / 写器 100 接收到的指令可以是请求读取存储在数据存储单元 205 上的预定数据的读取请求。

[0104] 在步骤 S29，CPU207 确定加密标记是否是 ON。如果在步骤 S29 中确定加密标记是 ON，则处理进行到步骤 S30。

[0105] 在步骤 S30，CPU207 分析在步骤 S25 中确定接收到的指令，执行预定的处理，并加密处理结果。在这种情况中，响应来自读 / 写器 100 的指令，读取存储在数据存储单元 205 的预定区域上的数据。加密处理器 208 加密所读取的数据。在加密处理中使用的加密秘密密钥是在步骤 S21 中产生的随机数。

[0106] 在步骤 S31，CPU207 向读 / 写器 100 发送在步骤 S30 中加密的数据。基于对发送的数据的解密，读 / 写器 100 读取存储在 IC 卡 200 上的数据。

[0107] 如果在步骤 S29 中确定出加密标记不是 ON，则处理进行到步骤 S32。

[0108] 在步骤 S32，CPU207 分析在步骤 S25 中确定接收到的指令，执行预定的处理，并发送处理得到的数据。响应来自读 / 写器 100 的指令，读取存储在数据存储单元 205 的预定区域上的数据。然后将读取的数据发送到读 / 写器 100。

[0109] 在上面讨论的处理中，从读 / 写器 100 接收读取存储在 IC 卡 200 上的数据的指令。当从读 / 写器 100 接收在 IC 卡 200 上存储（写入）数据的指令时，从读 / 写器 100 发送将要被写入的数据，然后将数据写入 IC 卡 200 上。

[0110] 由于在步骤 S32 中没有加密要发送的数据，所以读 / 写器 100 不需要对接收到的数据进行解密。如果还没有从读 / 写器 100 接收到发送卡 ID 的请求，则不将加密标记设置为 ON。不在读 / 写器 100 和 IC 卡 200 之间要通信的数据上进行加密。

[0111] 在步骤 S31 和 S32 的其中一个之后，处理回到步骤 S25。重复上述的处理直到 IC 卡 200 移出读 / 写器 100 的通信覆盖区域。

[0112] 由此执行 IC 卡 200 的通信处理。如果需要读 / 写器 100 提供的服务中的唯一识别单个 IC 卡的机构，则将卡 ID 加密并发送到 IC 卡 200。除了允许读取 IC 卡的卡 ID 的读 / 写器 100 之外的任何读 / 写器都不能获取卡 ID。因此通信系统 50 变成安全的和保护隐私的通信系统。

[0113] 不允许读 / 写器读取 IC 卡的卡 ID 但是遵照 NFCIP-1 标准的读 / 写器仍能够和 IC 卡 200 交换数据。当在读 / 写器 100 提供的服务中不需要唯一地识别单个 IC 卡时，每个 IC

卡可以没有任何问题地工作。

[0114] 在图 3 的例子中，启动器和目标的每一个都以 212kb/s 和 424kb/s 中的一个的数据传输率工作，并且使用通信 ID 作为 NFCID2。如果启动器和目标中的每一个都以 106kb/s 的数据传输率工作，则通信 ID 是 NFCIP-1 标准中定义的 NFCID1。

[0115] 下面参考图 4 的流程图具体描述读 / 写器 100 和 IC 卡 200 之间进行的通信处理。在允许读取 IC 卡 200 的卡 ID 的读 / 写器 100 和 IC 卡 200 之间进行的卡 ID 读取处理之后接着执行数据读取操作和数据写入操作。

[0116] 例如，靠近读 / 写器 100 的天线和放置 IC 卡 200，并将在 IC 卡 200 的天线中激励的 AC 磁场产生的电能馈送给 IC 卡 200 的每个部分。IC 卡 200 执行步骤 S101，由此产生随机数。

[0117] 下面参考图 5 的流程图描述在图 4 的步骤 S101 中进行的通信 ID 产生处理。

[0118] 在步骤 S301 中，随机数产生器 202 产生随机数 A。

[0119] 在步骤 S302 中，CPU207 将在步骤 S301 中产生的随机数 A 存储在数据存储单元 205 的预定区域中。

[0120] 在步骤 S303 中，加密处理器 208 使用存储在秘密密钥存储单元 203 上的密钥将在步骤 S301 中产生的随机数 A 加密。

[0121] 在步骤 S304 中，CPU207 将步骤 S303 中的处理结果（也就是加密的随机数 A）作为通信 ID 存储在数据存储单元 205 的预定区域上。

[0122] 在步骤 S301 到 S304 中进行的处理等同于在步骤 S21 和 S22 中进行的处理。

[0123] 回到图 4，在步骤 S201 中，读 / 写器 100 向读 / 写器 100 可以与其通信的 IC 卡 200 发送轮询请求。在步骤 S102 中，IC 卡 200 接收轮询请求。

[0124] 在步骤 S103 中，IC 卡 200 响应于在步骤 S102 中接收的轮询请求向读 / 写器 100 发送响应。如之前参考图 3 讨论的，将在步骤 S304 中在响应帧的预定区域中存储为 NFCID2 的通信 ID 嵌入将被发送到读 / 写器 100 的响应帧中。步骤 S102 和 S103 分别等同于图 2 的步骤 S23 和 S24。读 / 写器 100 在步骤 S202 中接收响应帧。

[0125] 在步骤 S203 中，读 / 写器 100 对从 IC 卡 200 发送的响应帧中的通信 ID 解密，由此获得随机数 A。

[0126] 下面参考图 6 的流程图描述在图 4 的步骤 S203 中执行的随机数产生处理。

[0127] 在步骤 S331 中，CPU105 获得包含在在步骤 S202 中从 IC 卡 200 接收到的响应帧中的通信 ID（也就是加密的随机数 A）。

[0128] 在步骤 S332 中，例如，CPU105 将在步骤 S331 中获得的通信 ID 存储在 RAM103 的预定区域上。

[0129] 在步骤 S333 中，加密处理器 106 使用存储在秘密密钥存储单元 101 上的密钥解密在步骤 S331 中获得的作为通信 ID 的随机数 A。如之前讨论的，加密处理器 106 根据与用于加密处理器 208 一样的算法执行加密处理或者解密处理。允许读取 IC 卡 200 的卡 ID 的读 / 写器 100 的秘密密钥存储单元 101 存储与存储在秘密密钥存储单元 203 上的密钥相同的密钥。在步骤 S333 中，由此解密和获得在步骤 S301 中通过 IC 卡 200 产生的随机数 A。

[0130] 在步骤 S334 中，CPU105 将在步骤 S333 中获得的随机数 A 存储在 RAM103 的预定区域上。

[0131] 读 / 写器 100 和 IC 卡 200 根据通信 ID 互相彼此识别，并根据需要使用随机数 A 作为密钥加密或者解密数据。由此在读 / 写器 100 和 IC 卡 200 之间交换通信需要的会话 ID（在这种情况中的通信 ID）和会话密钥（随机数 A）。

[0132] 回到图 4，在步骤 S204 中，读 / 写器 100 向 IC 卡 200 发送包含请求读取 IC 卡 200 的卡 ID 的指令的帧。在这种情况中，将在步骤 S332 中存储的通信 ID 嵌入帧中作为 IC 卡 200 的标识符以唯一地识别从读 / 写器 100 发送的帧。根据 NFCIP-1 标准，将通信 ID 嵌入在 NFCIP-1 标准中定义的转移帧（transfer frame）的传送数据字段中。在步骤 S104 中，IC 卡 200 接收该帧。

[0133] 在步骤 S105 中，IC 卡 200 执行响应于从读 / 写器 100 发送的指令的处理。在这种情况中，执行响应于读取卡 ID 的指令的处理。

[0134] 下面参考图 7 的流程图描述在图 4 的步骤 S105 中执行的卡 ID 发送处理。

[0135] 在步骤 S361 中，CPU207 读取存储在 ID 存储单元 204 上的卡 ID。

[0136] 在步骤 S362 中，加密处理器 208 使用在步骤 S302 中存储的随机数 A 加密在步骤 S361 中读取的卡 ID。

[0137] 在步骤 S363 中，CPU207 获取在步骤 S362 中的处理结果（加密的卡 ID）。

[0138] 回到图 4，在步骤 S105 之后的步骤 S106 中，IC 卡 200 发送包含在步骤 S363 中获得的数据的帧，作为响应于在步骤 S104 中从读 / 写器 100 读取卡 ID 的指令的响应。将在步骤 S304 中存储的通信 ID 嵌入为读 / 写器 100 的标识符以唯一地识别从 IC 卡 200 发送的帧。在步骤 S104 到 S106 中的处理等同于在步骤 S25 到 S28 中的处理。读 / 写器 100 在图 4 的步骤 S205 中读取该帧。

[0139] 由于响应于从读 / 写器 100 读取卡 ID 的指令读取卡 ID，所以在 IC 卡 200 中将加密标记设置为 ON（在图 2 的步骤 S27 中）。在随后的数据读取和写入处理中，以其加密的形式发送或者接收数据。

[0140] 在步骤 S206 中，读 / 写器 100 解密加密的卡 ID。

[0141] 下面参考图 8 的流程图描述图 4 的在步骤 S206 中的卡 ID 解密处理。

[0142] 在步骤 S391 中，CPU105 获得了包含在步骤 S205 中接收的帧中的加密数据。

[0143] 在步骤 S392 中，加密处理器 106 使用在步骤 S334 中存储的随机数作为密钥解密在步骤 S391 中获得的数据。

[0144] 在步骤 S393 中，CPU105 获取从步骤 S392 得到的数据作为卡 ID。以这种方式，读 / 写器 100 获得 IC 卡 200 的唯一卡 ID。读 / 写器 100 执行处理以提供使用卡 ID 的服务。

[0145] 回到图 4，读 / 写器 100 在步骤 S206 之后的步骤 S207 中向 IC 卡 200 发送帧。该帧包含读取存储在 IC 卡 200 上的数据（在由读 / 写器 100 提供的服务的处理所需的数据）的指令。将在步骤 S332 中存储的通信 ID 嵌入在帧中作为 IC 卡 200 的标识符以唯一地识别从读 / 写器 100 发送的帧。在步骤 S107 中，IC 卡 200 接收那个帧。

[0146] 在步骤 S108 中，IC 卡 200 响应于从读 / 写器 100 发送的指令执行处理，在这种情况中，执行响应于读取数据的指令的处理。

[0147] 下面参考图 9 的流程图描述在图 4 的步骤 S108 中执行的读取数据发送处理。

[0148] 在步骤 S421 中，CPU207 从存储在数据存储单元 205 上的数据读取读 / 写器 100 的所请求的数据。

[0149] 在步骤 S422 中，加密处理器 208 使用在步骤 S302 中存储的随机数 A 加密在步骤 S421 中读取的数据。

[0150] 在步骤 S423 中，CPU207 获取从步骤 S422 中得到的数据（加密的数据）。

[0151] 回到图 4，CPU207 在步骤 S109 中发送包含在步骤 S423 中得到的数据的帧，以此作为对在步骤 S107 中从读 / 写器 100 读取数据的指令的答复。在这种情况中，同样，将在步骤 S304 中存储的通信 ID 嵌入在帧中作为读 / 写器 100 的标识符，用以唯一地识别从 IC 卡 200 发送的帧。在步骤 S107 和 S108 中的处理等同于步骤 S25、S26 和 S29 到 S31 中的处理。在图 4 的步骤 S208 中，读 / 写器 100 接收那个帧。

[0152] 在步骤 S209 中，读 / 写器 100 解调从 IC 卡 200 接收到的数据。该处理等同于参考图 8 讨论的处理，并且不在这里重复对其具体的论述。在这个处理中，取而代之卡 ID 的是，使用随机数 A 解密由在读 / 写器 100 提供的服务的处理中需要的数据。

[0153] 在步骤 S210 中，读 / 写器 100 执行处理以使得 IC 卡 200 存储数据。

[0154] 下面参考图 10 的流程图描述图 4 的步骤 S210 中进行的写请求发送处理。

[0155] 在步骤 S451 中，CPU105 获取从读 / 写器 100 执行的应用程序得到的数据并存储到 IC 卡 200 上。

[0156] 在步骤 S452 中，加密处理器 106 使用在步骤 S334 中存储的随机数 A 对在步骤 S451 中得到的数据加密。

[0157] 在步骤 S453 中，CPU105 将从步骤 S452 得到的数据（加密的数据）和写请求指令一起存储在帧中。

[0158] 回到图 4，读 / 写器 100 在步骤 S210 之后的步骤 S211 中将包含在步骤 S453 中加密的数据的写请求的帧发送到 IC 卡 200。还将在步骤 S332 中存储的通信 ID 作为 IC 卡 200 的标识符嵌入，以唯一地识别从读 / 写器 100 发送的帧。在步骤 S110 中，IC 卡 200 接收那个帧。

[0159] 在步骤 S111 中，IC 卡 200 执行响应于从读 / 写器 100 发送的指令的处理。执行响应于数据写指令的处理。

[0160] 下面参考图 11 的流程图描述在图 4 的步骤 S111 中执行的数据写处理。

[0161] 在步骤 S481 中，CPU207 获取包含在步骤 S110 中接收到的帧中的加密数据。

[0162] 在步骤 S482 中，加密处理器 208 用在步骤 S302 中存储的随机数 A 加密在步骤 S481 中获得的数据。

[0163] 在步骤 S483 中，CPU207 将从步骤 S482 得到的数据（加密的数据）存储到数据存储单元 205 的预定区域上，由此执行写处理。

[0164] 回到图 4，IC 卡 200 在步骤 S111 之后的步骤 S112 中将包含从步骤 S483 得到的数据的帧发送到读 / 写器 100。发送的帧包含表示数据是否被成功写入的数据。还将在步骤 S304 中存储的通信 ID 作为读 / 写器 100 的标识符嵌入在帧中，用以唯一地识别从 IC 卡 200 发送的帧。在步骤 S212 中，读 / 写器 100 接收那个帧。

[0165] 读取卡 ID 之后，进行数据读取然后进数据写入。数据读取和数据写入不局限于这种顺序。根据需要可以改变该顺序。

[0166] 由此在 IC 卡 200 和允许读取读 / 写器 100 的卡 ID 的读 / 写器 100 之间进行通信。将加密的卡 ID 发送到读 / 写器 100，并在卡 ID 读取之后进行的数据读取和数据写入中加密

所有的数据。通信系统 50 由此变得安全并且不会侵犯用户隐私。

[0167] 用存储在秘密密钥存储单元 101 和秘密密钥存储单元 203 上的密钥可以加密所通信的数据。为了以安全方式发送和接收数据，每个 IC 卡需要具有不同的秘密密钥。结果，强制读 / 写器 100 记住用于各个 IC 卡的大量密钥，并难于管理密钥。

[0168] 根据本发明的一个实施例，不仅在读 / 写器 100 和 IC 卡 200 之间交换作为会话 ID（标识符）的通信 ID，还要在读 / 写器 100 和 IC 卡 200 之间共享通过解密通信 ID 获得的随机数 A，而不需要第三方的任何知识。在每次 IC 卡 200 和读 / 写器 100 通信时产生随机数 A。如果预先进行这样的安排，即将随机数 A 用作在随后的通信中加 密或者解密的密钥，则在每次进行通信时使用不同的会话密钥进行加密通信。由此在不需要在读 / 写器 100 上为单独的 IC 卡存储大量的秘密密钥数据的条件下进行用会话秘密密钥的加密。通信系统 50 变成具有简单设计的安全系统。

[0169] 不允许读取 IC 卡 200 的卡 ID 的读 / 写器不存储与秘密密钥存储单元 203 上所存储的密钥相同的密钥。即使读 / 写器作出卡 ID 发送请求，也没有从通信 ID 解密随机数，并且不能通过解密用随机数作为密钥加密的形式发送的卡 ID 而获得卡 ID。

[0170] 根据本发明的一个实施例。读 / 写器 100（启动器）和 IC 卡 200（目标）只遵照 NFCIP-1 标准进行通信，不需要执行任可附加的处理，例如用于会话密钥交换的握手协议。

[0171] NFCIP-1 标准将 NFC 标识符（例如图 3 的 NFCID2）的用途定义为 NFC 装置标识符，其使用冲突避免和单一装置检测处理的随机数。随机数产生器 202（或者等效的元件）最初包含在遵照 NFCIP-1 标准的 IC 卡 200 中。本发明的实施例中使用的通信 ID 只是在目标中产生的加密随机数。重新安排了加密处理，但是没有必要在作为会话 ID 的通信 ID 交换中引入附加的处理。

[0172] 根据本发明的一个实施例，使用通过解密通信 ID 获得的随机数作为会话密钥。当从遵照 NFCIP-1 标准的启动器发送轮询请求和从目标发送轮询响应时，一起交换会话秘密密钥和通信 ID。不需要任何附加的处理。

[0173] 根据本发明的实施例，IC 卡 200 可以在不知道读 / 写器类型（也就是，关于该读 / 写器是特殊的读 / 写器还是通用读 / 写器）的情况下执行处理。特殊的读 / 写器是允许读取 IC 卡的卡 ID 并以其加密的形式传输的数据读 / 写器。通用读 / 写器是不允许读取 IC 卡的卡 ID 和传输没有加密的数据的读 / 写器。如果读 / 写器起到遵照 NFCIP-1 标准的启动器的作用，本发明的一个实施例的 IC 卡可以没有任何问题地和读 / 写器通信。因此 IC 卡 200 提供了装置的兼容性。

[0174] 下面参考图 12 的流程图描述在本发明的一个实施例的 IC 卡 200 和通用读 / 写器（未示出）之间执行的通信处理。不允许通用读 / 写器读取 IC 卡 200 的卡 ID。在这种通信处理中，在不加密的情况下交换数据。

[0175] 步骤 S121 到 S123 分别等同于图 4 的步骤 S101 到 S103。步骤 S221 和 S222 分别等同于图 4 的步骤 S201 和 S202。

[0176] 不同于图 4 的顺序，在图 12 的处理中，读 / 写器不解密包含在步骤 S222 中从 IC 卡 200 接收到的响应中的通信 ID。没有将读取卡 ID 的请求从读 / 写器发送到 IC 卡 200，并不从 IC 卡 200 发送响应。更特别地，不以图 12 的顺序执行对应于图 4 的步 骤 S203 到 S205 以及步骤 S104 到 S106 的处理。

[0177] 由于读/写器没有发出读取卡 ID 的请求，所以 IC 卡 200 不将加密标记设置为 ON（没有执行图 2 的步骤 S27），并在随后的数据读取和数据写入处理中不加密数据。

[0178] 不以图 12 的顺序执行对应于图 4 的步骤 S108、S209、S210 和 S111 的处理。在步骤 S129 和 S231 中，发送没有加密的读取数据和写入数据，在步骤 S228 和 S130 中，在没有解密的情况下获取或者存储接收到帧的数据。步骤 S129 和 S131 中的处理等同于图 2 的步骤 S32 中的处理。

[0179] 如图 12 所示，在步骤 S227、S129、S231 和 S131 的每一个中发送的帧中，也将在步骤 S121 中产生的通信 ID 嵌入作为标识符。

[0180] 本发明的实施例的 IC 卡 200 可以和通用读/写器一起使用并提供装置的兼容性，由此保持通信系统的低成本。

[0181] 根据之前的实施例，使用存储在 IC 卡 200 中的秘密密钥加密在 IC 卡 200 中产生的随机数 A，然后将加密的随机数 A 作为通信 ID 发送到读/写器 100。读/写器 100 和 IC 卡 200 使用随机数 A 互相识别和进行数据加密通信。

[0182] 将通信 ID 存储在通过 NFCIP-1 标准定义的响应帧中用于 NFCID2 的 8 字节字段中。将通信 ID 和随机数 A 的每一个限定到最大 8 字节（64 位）的数据长度。

[0183] 在作为加密算法的 2-Key Triple-DES 中，密钥的数据长度是 112 位。为了发送关于 112 位密钥的信息，需要至少 112 位的数据长度。在作为加密算法的高级加密标准（AES）中，秘密密钥的数据长度最小是 128 位。为了发送关于 128 位的密钥的信息，需要至少 128 位的数据长度。

[0184] 如果采用 2-Key Triple-DES 或 AES 作为加密算法，轮询请求的单个响应不能发送产生用于加密通信的密钥所需要的所有信息。必要的是，读/写器 100 将包含询问有关信息缺少的指令的帧发送给 IC 卡 200，IC 卡 200 答复响应。除了图 4 的过程之外，还需要在读/写器 100 和 IC 卡 200 之间进行交换剩余的信息的附加处理。

[0185] 在图 13 的通信系统 500 中，即使在预定加密算法中使用的密钥的数据长度是 128 位时，也不需要在读/写器 100 和 IC 卡 200 之间进行交换用于补偿缺少的密钥信息的剩余信息的通信。

[0186] 图 13 是示出了根据本发明的一个实施例的通信系统 500 的方框图。如图所示，用相同的附图标记表示等同于在之前实施例中描述的那些元件，并适当地省略对其的论述。

[0187] 通信系统 500 包括读/写器 600 和 IC 卡 200。在通信系统 500 中，与在通信系 统 50 中使用的相同 IC 卡 200 和读/写器 600 进行无线通信。

[0188] 读/写器 600 包括分别与图 1 的读/写器 100 的其相对部分（counterpart）相同的秘密密钥存储单元 601、输入输出单元 602、RAM603、ROM604、CPU605 和加密处理器 606。读/写器 600 还包括随机数产生器 607 和数据存储单元 608。

[0189] 与 IC 卡 200 中的随机数产生器 202 类似，随机数产生器 607 根据需要产生预定数字的随机数。例如，随机数产生器 607 产生 8 字节长的随机数 B。数据存储单元 608 存储需要存储在与 IC 卡 200 的通信中的数据。例如，数据存储单元 608 存储通过随机数产生器 607 产生的随机数 B。

[0190] 如上述的通信系统 50，IC 卡 200 在通信系统 500 中产生 8 字节的随机数 A。IC 卡 200 向读/写器 600 发送用通信 ID 加密的随机数 A。读/写器 600 还产生 8 字节长的随机

数 B，并向 IC 卡 200 发送用秘密密钥加密的随机数 B。结果，读 / 写器 600 和 IC 卡 200 中的每一个都可以共享包括源自于本身装置的 8 字节随机数和从通信伙伴装置接收到的另一个 8 字节随机数的 16 字节随机数。读 / 写器 600 和 IC 卡 200 中的每一个都采用 16 字节（182 位）的随机数作为会话密钥。

[0191] 如在图 4 的通信处理中，读 / 写器 600 在 IC 卡 200 上执行数据读取和数据写入。将来自读 / 写器 600 的加密随机数 B 以下述两种方法发送到 IC 卡 200。在第一种方法中，将加密的随机数 B 作为轮询请求的附带信息 (incidental information) 发送。在第二种方法中，将加密的随机数 B 作为轮询请求之后发送的帧的附带信息发送。轮询请求帧和轮询请求帧之后的帧（包含请求读取卡 ID 的指令）中的每一个都包含用于存储至少 8 位长数据的空区域（可扩展的）。

[0192] 图 14 是在读 / 写器 600 和 IC 卡 200 之间进行的通信处理的流程图。在通信处理中，将加密随机数 B 从读 / 写器 600 发送到 IC 卡 200，作为轮询请求的附带信息。

[0193] 可以将 IC 卡 200 放置在读 / 写器 600 的天线附近，并将在输入输出单元 201 的天线中激励的 AC 磁场产生的电能馈送给 IC 卡 200 的每个部分。IC 卡 200 执行步骤 S601，由此产生 8 字节的随机数 A。步骤 S601 等同于参考图 5 讨论的通信 ID 产生处理，这里不再讨论。

[0194] 读 / 写器 600 执行步骤 S501，由此产生包含附带信息的轮询帧。

[0195] 下面参考图 15 的流程图描述在图 14 的步骤 S501 中进行的轮询请求产生处理。

[0196] 在步骤 S701 中，随机数产生器 607 产生 8 字节的随机数 B。

[0197] 在步骤 S702 中，CPU605 将在步骤 S701 中产生的随机数 B 存储在数据存储单元 608 的预定区域上。

[0198] 在步骤 S703 中，加密处理器 606 使用存储在秘密密钥存储单元 601 上的密钥对在步骤 S701 中产生的随机数 B 加密。

[0199] 在步骤 S704 中，CPU605 将从步骤 S703 得到的数据（也就是加密的随机数 B）作为轮询请求的附带信息存储在数据存储单元 608 的预定区域上。

[0200] 回到图 14，读 / 写器 600 在步骤 S502 向 IC 卡 200 发送包含附带信息的轮询请求。在步骤 S602 中，IC 卡 200 接收轮询请求。

[0201] 在步骤 S603 中，IC 卡 200 对从读 / 写器 600 接收到的轮询请求的附带信息解密，由此获得随机数 B。

[0202] 下面参考图 16 的流程图描述在图 14 的步骤 S603 中进行的随机数 B 获取处理。

[0203] 在步骤 S731 中，CPU207 获取包含在步骤 S602 中从读 / 写器 600 接收到的轮询请求中的附带信息（也就是，加密的随机数 B）。

[0204] 在步骤 S732 中，CPU207 将在步骤 S731 中获得的附带信息存储在数据存储单元 205 的预定区域上。

[0205] 在步骤 S733 中，加密处理器 208 使用存储在秘密密钥存储单元 203 上的密钥解密加密的随机数 B，也就是包含在步骤 S731 中得到的轮询请求中的附带信息。由此获得随机数 B

[0206] 在步骤 S734 中，CPU207 将在步骤 S733 中得到的随机数 B 存储在数据存储单元 205 的预定区域上。

[0207] 回到图 14，IC 卡 200 在步骤 S604 中将响应于在步骤 S602 中接收到的轮询请求的响应发送给读 / 写器 600。将在步骤 S601 中产生的通信 ID（也就是，加密的随机数 A）存储为包含在响应帧的预定区域中的 NFCID2（见图 3）。读 / 写器 600 在步骤 S503 接收响应帧。

[0208] 在步骤 S504 中，读 / 写器 600 通过解密从 IC 卡 200 接收到的响应帧的通信 ID 获得随机数 A。步骤 S504 等同于参考图 6 讨论的随机数获取处理，这里不再讨论。

[0209] 读 / 写器 600 和 IC 卡 200 现在已经交换了当前通信（会话）中需要的会话 ID（也就是，通信 ID）和会话密钥（也就是，8 字节随机数 A 和 8 字节随机数 B）。

[0210] 在步骤 S504 之后，将唯一地识别读 / 写器 600 和 IC 卡 200 中的每一个作为通信伙伴的通信 ID 嵌入在读 / 写器 600 和 IC 卡 200 之间通信的每一个帧中。在读 / 写器 600 和 IC 卡 200 之间通信的帧包含包括用具有 8 字节随机数 A 和 8 字节随机数 B 的 16 字节会话秘密密钥加密的数据。

[0211] 对包含读取卡 ID 的请求指令、读取数据的请求指令和在步骤 S504 之后通过读 / 写器 600 进行的写数据的请求指令的帧以及响应于帧由 IC 卡 200 进行的答复的发送分别等同于之前参考图 4 讨论的在读 / 写器 100 和 IC 卡 200 之间进行的对应部分。更特别地，图 14 的步骤 S505 到 S513 分别等同于图 4 的步骤 S204 到 S212。图 14 的步骤 S605 到 S613 分别等同于图 4 的步骤 S104 到 S112。图 4 的处理和图 14 的处理之间的区别是用随机数 A 和随机数 B 的组合（16 字节会话密钥）而不是用随机数 A（8 字节会话密钥）加密包含在读 / 写器 600 和 IC 卡 200 之间发送的帧中的数据。

[0212] 图 17 是在读 / 写器 600 和 IC 卡 200 之间进行的通信处理的流程图。在通信处理中，将加密的随机数 B 从读 / 写器 600 发送到 IC 卡 200，作为轮询请求之后发送到帧的附带信息。

[0213] 如图 17 所示，IC 卡 200 产生 8 字节随机数 A，并响应来自读 / 写器 600 的轮询请求将加密随机数 A 作为通信 ID 发送到读 / 写器 600。读 / 写器 600 接收和解密通信 ID，由此获得 8 字节随机数 A。迄今进行的处理等同于参考图 4 讨论的读 / 写器 100 和 IC 卡 200 之间进行的处理。更特别地，由读 / 写器 600 进行的图 17 的步骤 S531 到 S533 分别等同于图 4 的步骤 S201 到 S203。由 IC 卡 200 进行的图 17 的步骤 S641 到 S643 分别等同于图 4 的步骤 S101 到 S103。

[0214] 作为唯一地识别读 / 写器 600 和 IC 卡 200 的每一个作为通信伙伴的标识符，通信 ID 被嵌入在读 / 写器 600 和 IC 卡 200 之间在下文中通信的每一帧中。

[0215] 在步骤 S533 中，读 / 写器 600 将通信 ID 存储在 RAM103 的预定区域上并解密通信 ID 以获得随机数 A。在步骤 S534 中，读 / 写器 600 产生读取具有附在其上的附带信息的卡 ID 的请求。

[0216] 下面参考图 18 的流程图描述图 17 的步骤 S534 中进行的卡 ID 读取请求产生处理。

[0217] 在步骤 S761 中，随机数产生器 607 产生随机数 B。

[0218] 在步骤 S762，CPU605 将在步骤 S761 中产生的随机数 B 存储在数据存储单元 608 的预定区域上。

[0219] 在步骤 S763 中，加密处理器 606 使用存储在秘密密钥存储单元 601 上的密钥将在

步骤 S761 产生的随机数 B 加密。

[0220] 在步骤 S764 中，CPU605 将从步骤 S763 得到的数据（也就是加密的随机数 B）作为 ID 读取请求的附带信息存储在数据存储单元 608 的预定区域上。

[0221] 回到图 17，读 / 写器 600 在步骤 S535 中将包含请求读取具有附在其上的附带信息的卡 ID 的指令的帧发送到 IC 卡 200。在步骤 S644 中，IC 卡 200 接收那个帧。

[0222] 在步骤 S645 中，IC 卡 200 解密从读 / 写器 600 接收到的 IC 卡读取请求的附带信息，由此获得随机数 B。

[0223] 下面参考图 19 的流程图描述在图 17 的步骤 S645 中进行的随机数 B 获取处理。

[0224] 在步骤 S791 中，CPU207 获取包含在步骤 S644 中从读 / 写器 600 接收到的卡 ID 读请求中的附带信息（也就是随机数 B）。

[0225] 在步骤 S792 中，CPU207 将在步骤 S791 中获得的附带信息存储在数据存储单元 205 的预定区域上。

[0226] 在步骤 S793 中，加密处理器 208 使用存储在秘密密钥存储单元 203 上的密钥解密经加密的随机数 B，也就是，包含在步骤 S791 中获得的卡 ID 读取请求的附带信息。由此获得随机数 B。

[0227] 在步骤 S794 中，CPU207 将在步骤 S793 中获得的随机数 B 存储在数据存储单元 205 的预定区域上。

[0228] 通过上述处理，读 / 写器 600 和 IC 卡 200 已经交换了会话 ID（通信 ID）和执行当前通信所需的会话密钥 (8 字节随机数 A 和 8 字节随机数 B)。

[0229] 除了用随机数 A 和随机数 B 的组合 (16 字节会话密钥）而不是用随机数 A(8 字节会话密钥）加密包含在读 / 写器 600 和 IC 卡 200 之间发送的帧中的数据之外，在图 17 中所示的由 IC 卡 200 执行的步骤 S646 到 S653 以及由读 / 写器 600 执行的步骤 S536 到 S542 分别等同于图 4 的步骤 S105 到 S112 和步骤 S205 到 S212。

[0230] 在如上所述的通信系统 500 中，读 / 写器 600 用秘密密钥对由随机数产生器 607 产生的 8 字节随机数 B 加密，然后将在轮询帧中作为附带信息的加密随机数 B 或者轮询帧之后的下一帧中的加密随机数 B 发送到 IC 卡 200。IC 卡 200 用秘密密钥将由随机数产生器 202 产生的随机数 A 加密并将加密的随机数 A 作为通信 ID 发送到读 / 写器 600。

[0231] 读 / 写器 600 和 IC 卡 200 中的每一个都共享包含由自身装置产生的 8 字节长随机数 A（随机数 B）和由通信伙伴产生的 8 字节长随机数 B（随机数 A）的组合的 16 字节 (128 位）长密钥。

[0232] 本发明的实施例的通信系统可以以加密算法运行，例如需要 112 位或者 128 位密钥数据长度的 2-Key Triple-DES 或者 AES。由对图 4 的流程图和图 17 的流程图的比较可见，在读 / 写器 600 和 IC 卡 200 之间进行的通信帧的数量（通信会话的数量）等同于在通信系统 50 中进行的通信帧数量。更特别地，为了共用 16 字节长密钥，通信系统 50 需要询问有关信息不足的附加通信，而通信系统 500 可以没有这样的附 加通信步骤。

[0233] 利用通信帧的最小数量，通信系统 500 与使用具有比通信 ID 的数据长度更长数据长度的密钥的加密系统兼容。

[0234] 在上述的讨论中，由读 / 写器 600 产生的随机数 B 的数据长度是 8 字节长。取决于存储附带信息的帧的空区域，可以将随机数 B 的数据长度设置为大于 8 字节。可以将在

读 / 写器 600 和 IC 卡 200 中的每一个中使用的会话密钥设置为大于 128 位。

[0235] 如上面参考图 2 所述的，当发出卡 ID 发送请求时，在之前实施例中将加密标记设置为 ON。为了以其加密的形式通信数据，读 / 写器 600 将卡 ID 发送请求发送给 IC 卡 200。

[0236] 即使需要将传输的数据保密，也可能不需要卡 ID。在这种情况中，可以独立地安排将加密标记设置为 ON 的指令，并从读 / 写器 600 发送到 IC 卡 200。更特别地，参考图 14 和图 17 的处理，代替卡 ID 读取请求指令，将包含将加密标记设置为 ON 的指令的帧从读 / 写器 600 发送到 IC 卡 200。为了一直对数据加密，在交换会话密钥之后，总是解密读 / 写器 600 和 IC 卡 200 之间传输的数据（加密标记保持为 ON）。在这种情况中，可以消除加密标记。

[0237] 已经讨论了包含 IC 卡和读 / 写器的通信系统。本发明还可应用于包含 NFCIP-1 启动器和 NFCIP-1 目标的系统，例如 RFID 和 RFID 读取器。

[0238] 可以使用硬件或软件执行上述处理的一系列处理。如果使用软件执行这一系列处理步骤，则通过图 1 的 CPU105 和 CPU207 的其中一个执行形成该软件的程序。读 / 写器 100 和 IC 卡 200 的其中一个从可读记录介质读取程序。

[0239] 可以以上述的时间序列顺序执行上述的一系列处理。可替换地，可以并行地或者分别地执行这一系列处理步骤。

[0240] 本领域技术人员应当理解的是，可以根据设计需求和其它的因素进行各种改变、组合、子组合和替换，只要它们落在附带的权利要求或者其等价范围内。

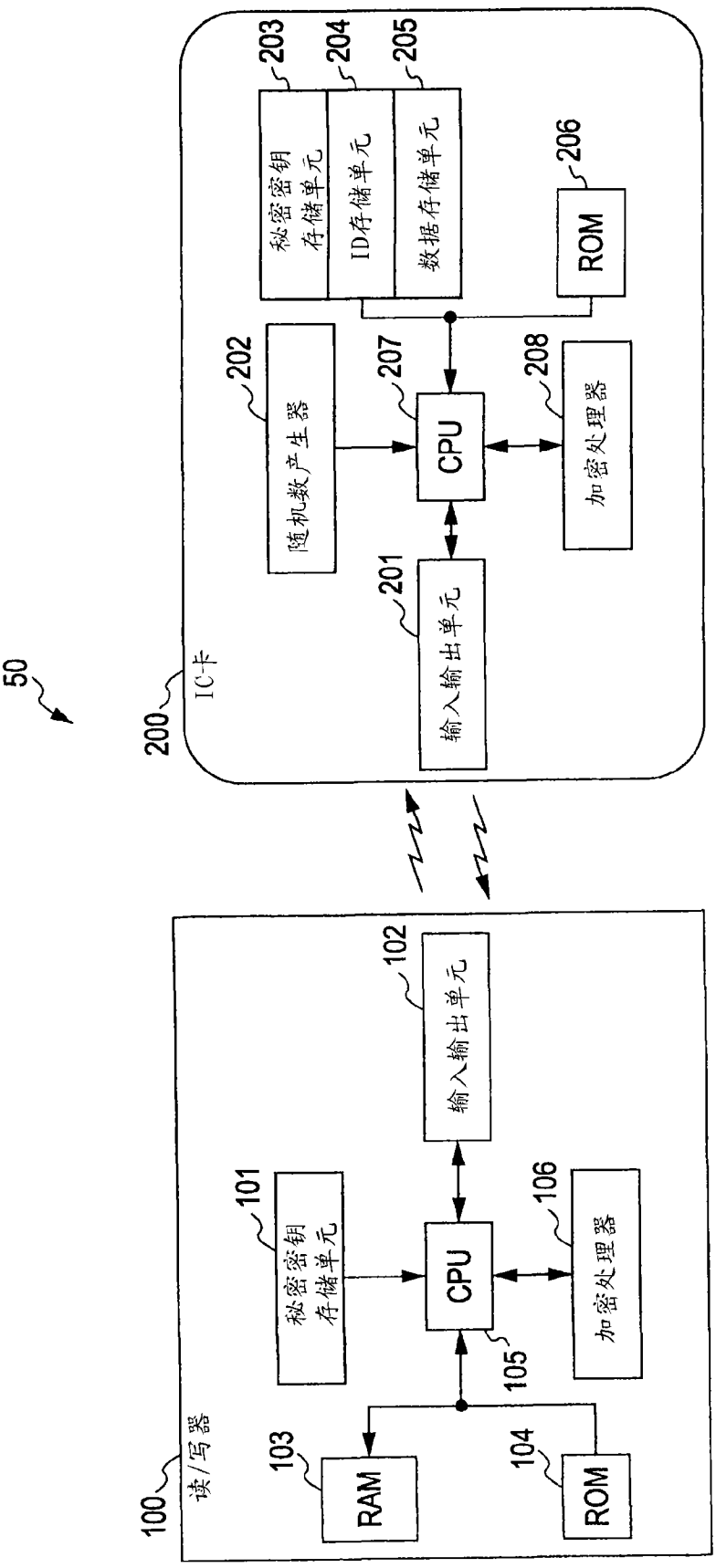

50
200
IC卡
201
输入输出单元
202
随机数产生器
203
秘密密钥存储单元
204
ID存储单元
205
数据存储单元
206
ROM
207
CPU
208
加密处理器
100
读/写器
101
秘密密钥存储单元
102
输入输出单元
103
RAM
104
ROM
105
CPU
106
加密处理器

图 1

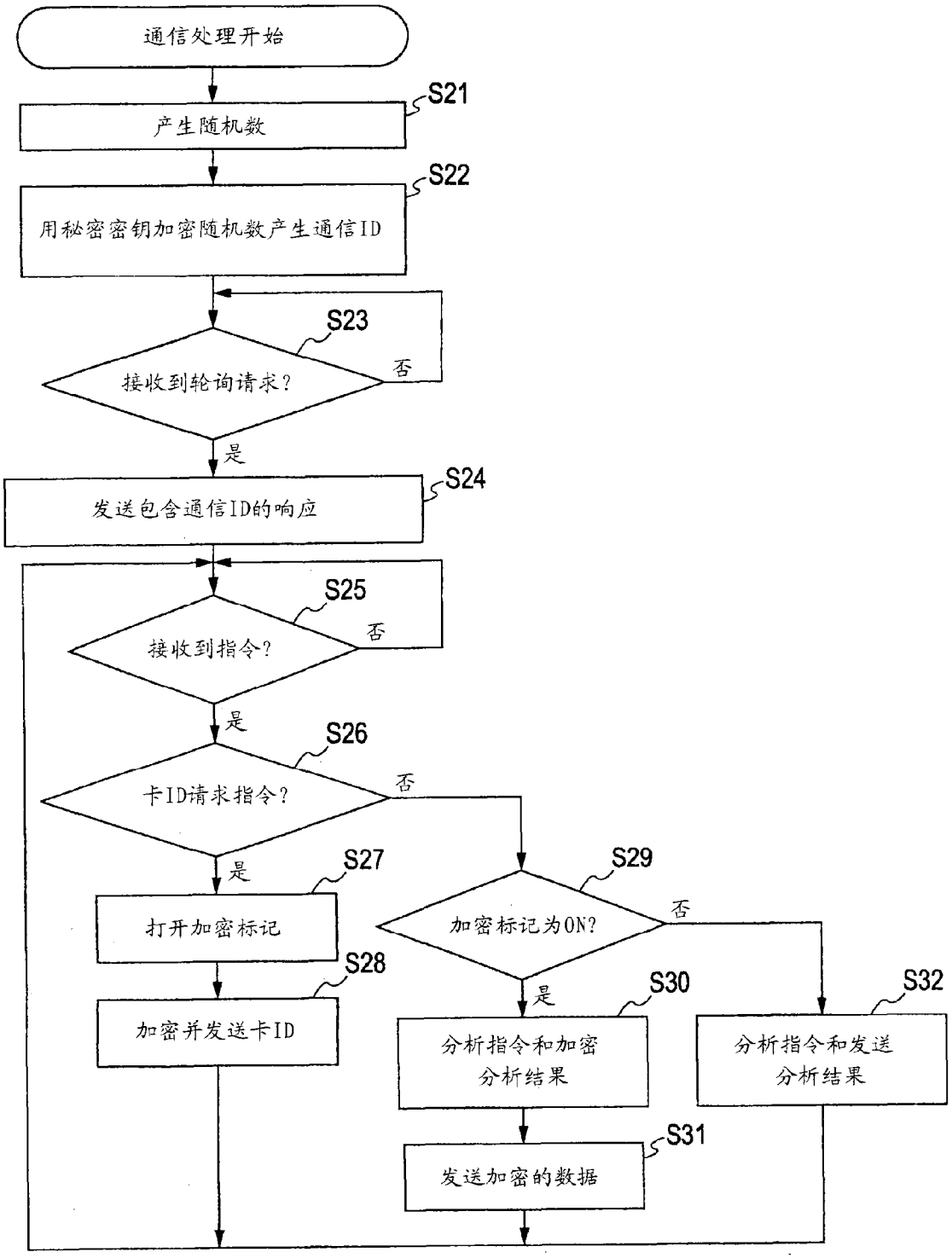

通信处理开始
S21
产生随机数
S22
用秘密密钥加密随机数产生通信ID
S23
接收到轮询请求?
否
是
S24
发送包含通信ID的响应
S25
接收到指令?
否
是
S26
卡ID请求指令?
否
是
S27
打开加密标记
S28
加密并发送卡ID
S29
加密标记为ON?
否
是
S30
分析指令和加密
分析结果
S32
分析指令和发送
分析结果
S31
发送加密的数据

图 2

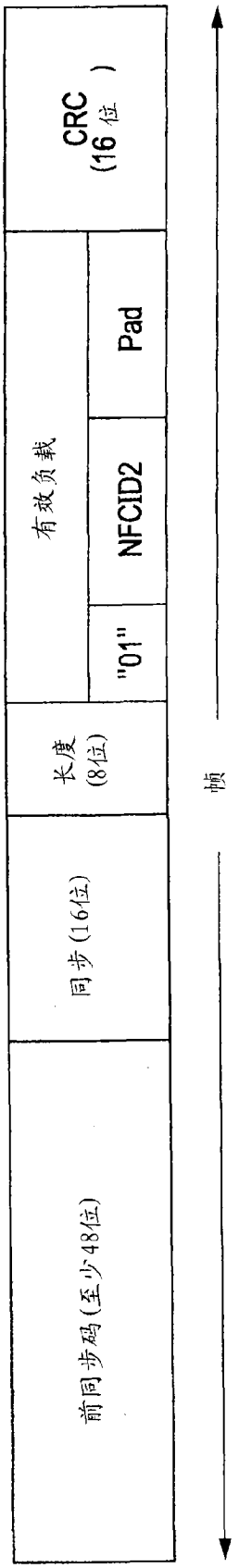


图 3

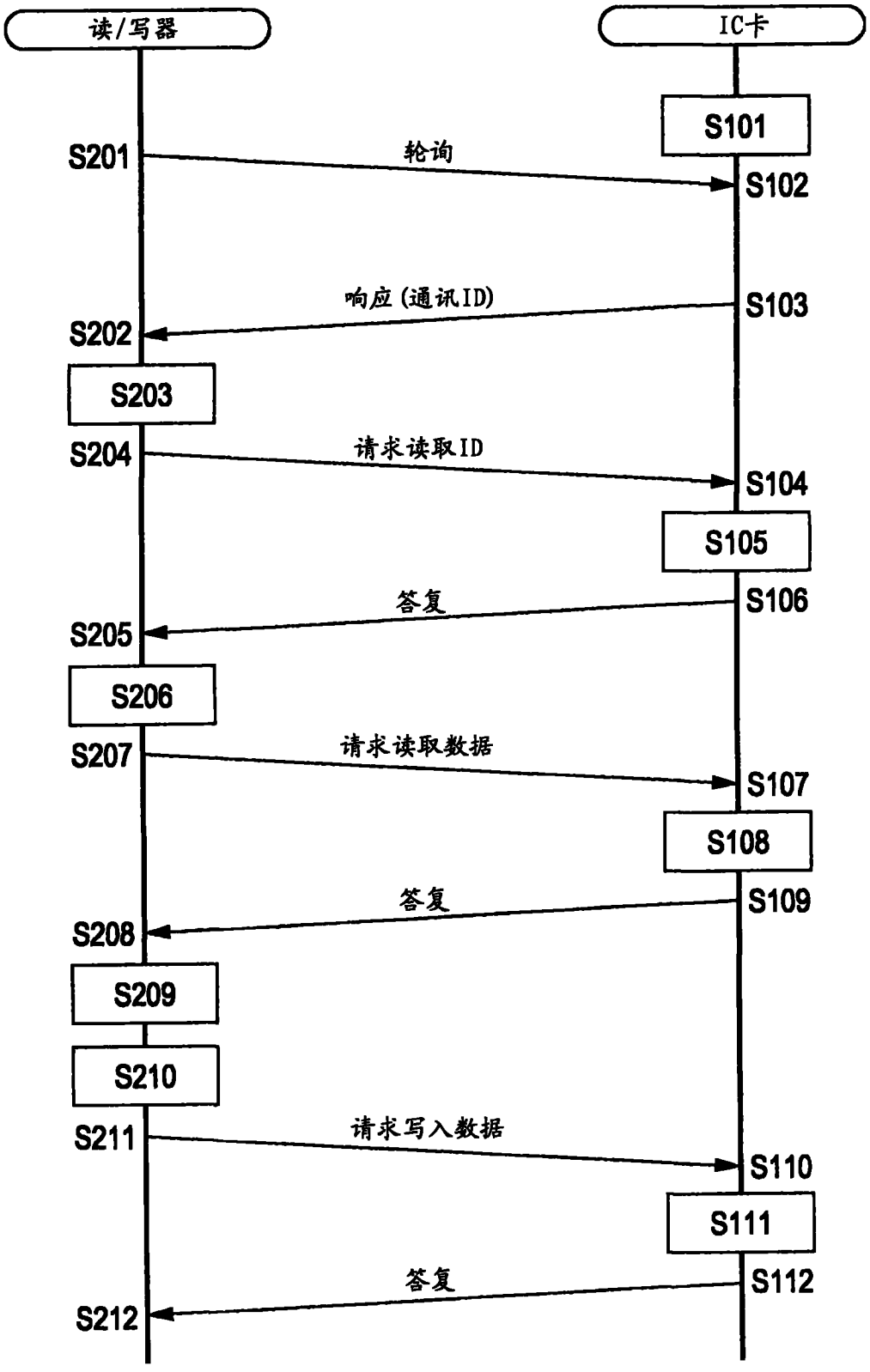

读/写器
IC卡
S101
S201
轮询
S102
响应(通讯ID)
S103
S202
S203
S204
请求读取ID
S104
S105
答复
S106
S205
S206
S207
请求读取数据
S107
S108
答复
S109
S208
S209
S210
S211
请求写入数据
S110
S111
答复
S112
S212

图 4

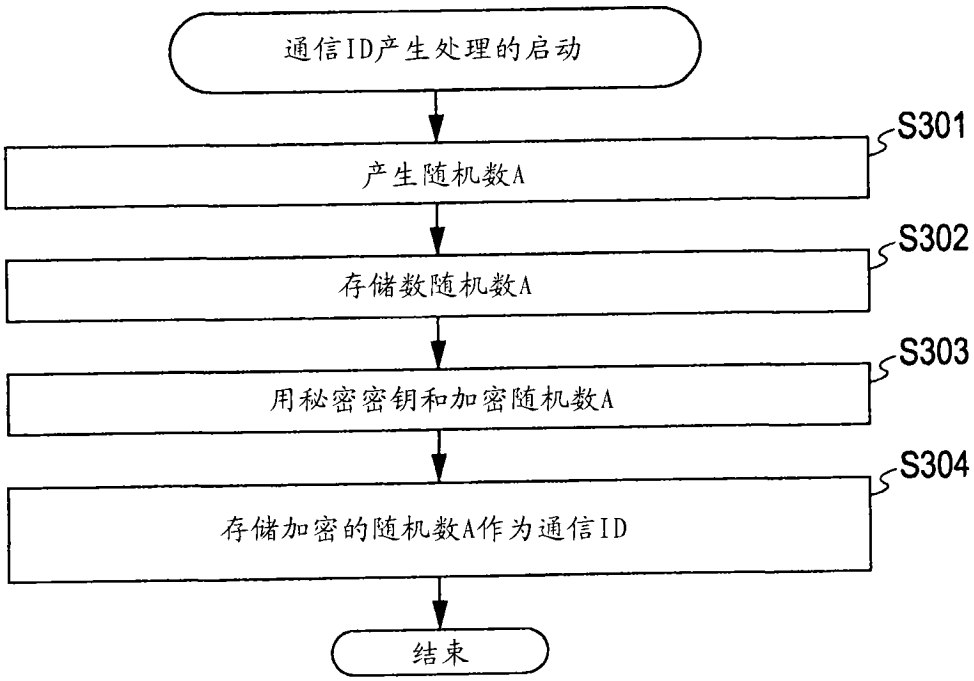

通信ID产生处理的启动
S301
产生随机数A
S302
存储数随机数A
S303
用秘密密钥和加密随机数A
S304
存储加密的随机数A作为通信ID
结束

图 5

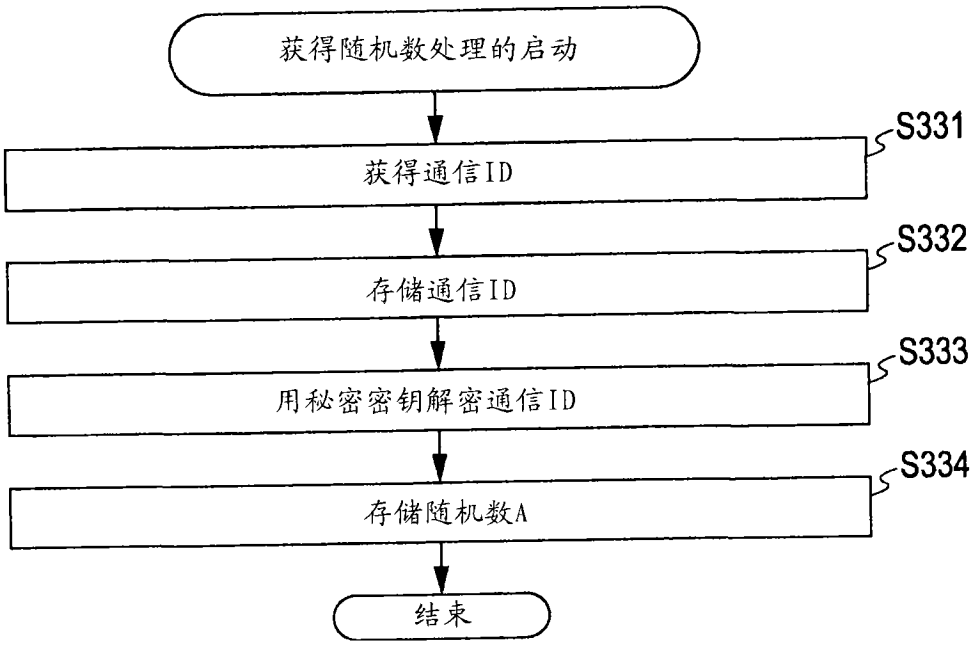

获得随机数处理的启动
S331
获得通信ID
S332
存储通信ID
S333
用秘密密钥解密通信ID
S334
存储随机数A
结束

图 6

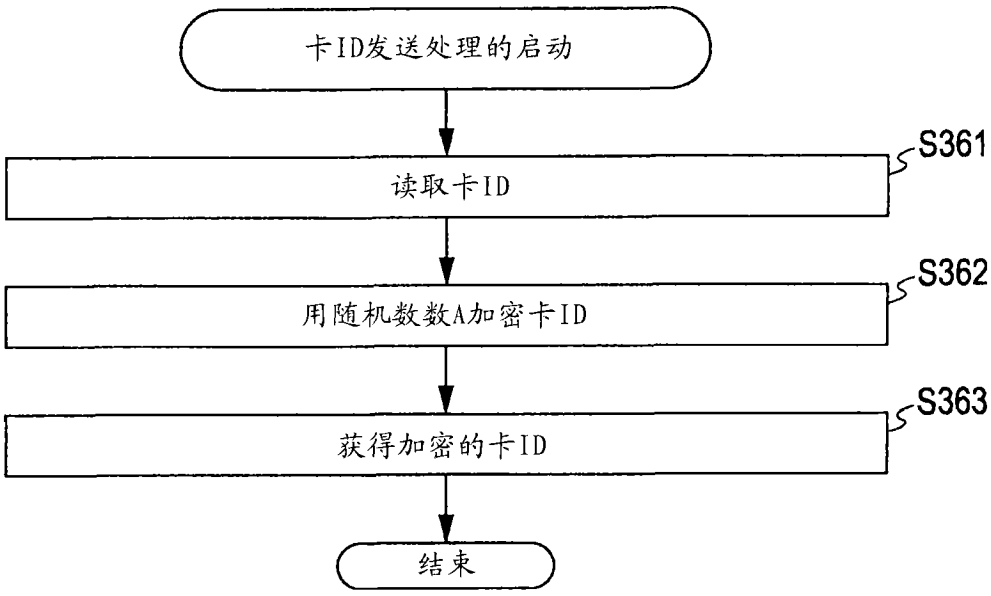

卡ID发送处理的启动
S361
读取卡ID
S362
用随机数数A加密卡ID
S363
获得加密的卡ID
结束

图 7

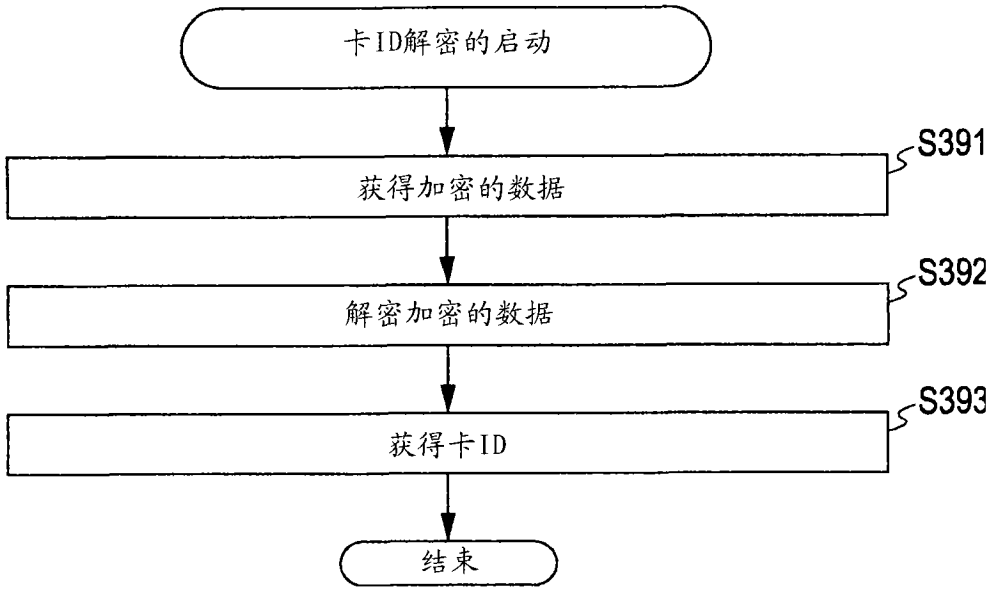

卡ID解密的启动
S391
获得加密的数据
S392
解密加密的数据
S393
获得卡ID
结束

图 8

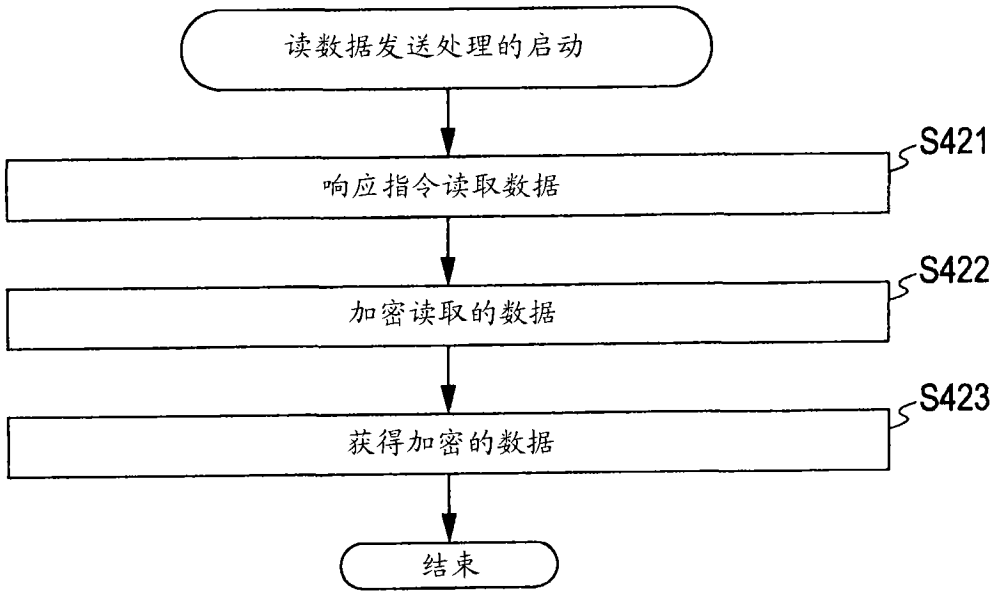

读数据发送处理的启动
S421
响应指令读取数据
S422
加密读取的数据
S423
获得加密的数据
结束

图 9

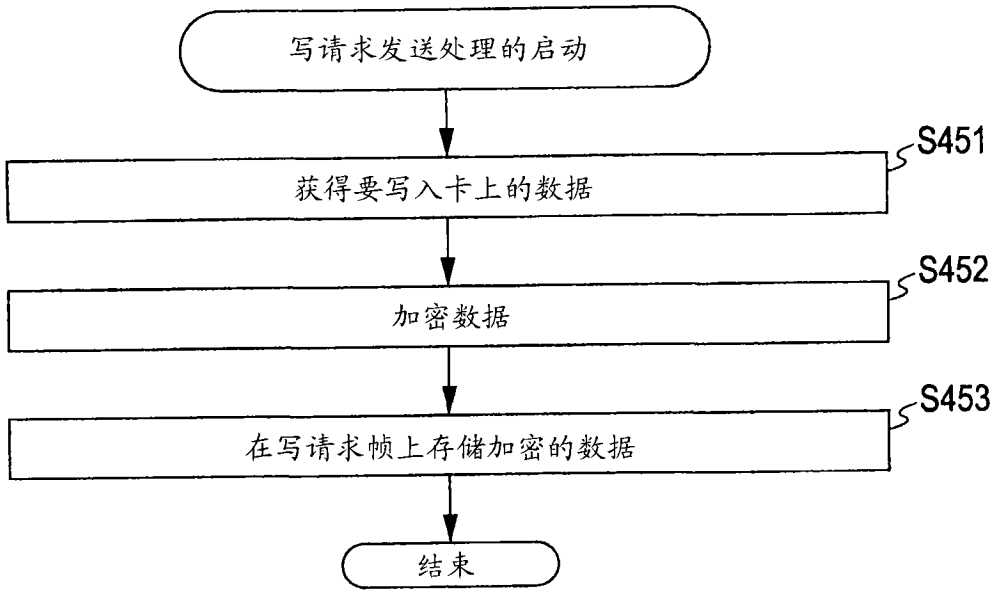

写请求发送处理的启动
S451
获得要写入卡上的数据
S452
加密数据
S453
在写请求帧上存储加密的数据
结束

图 10

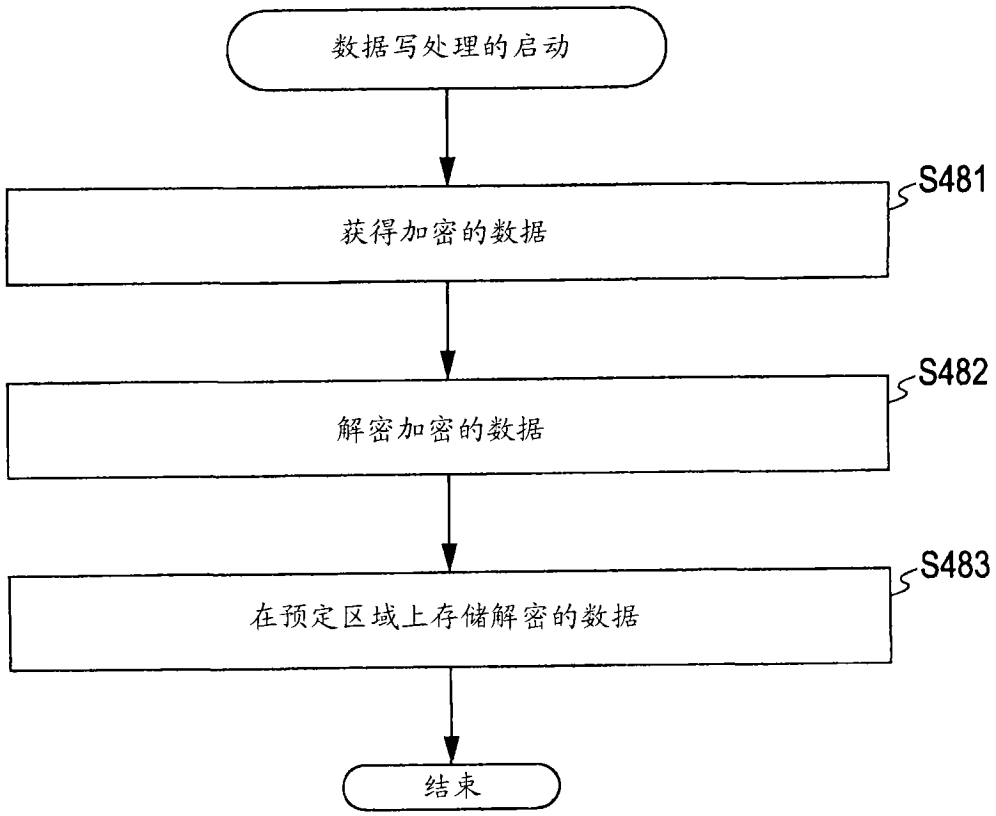


图 11

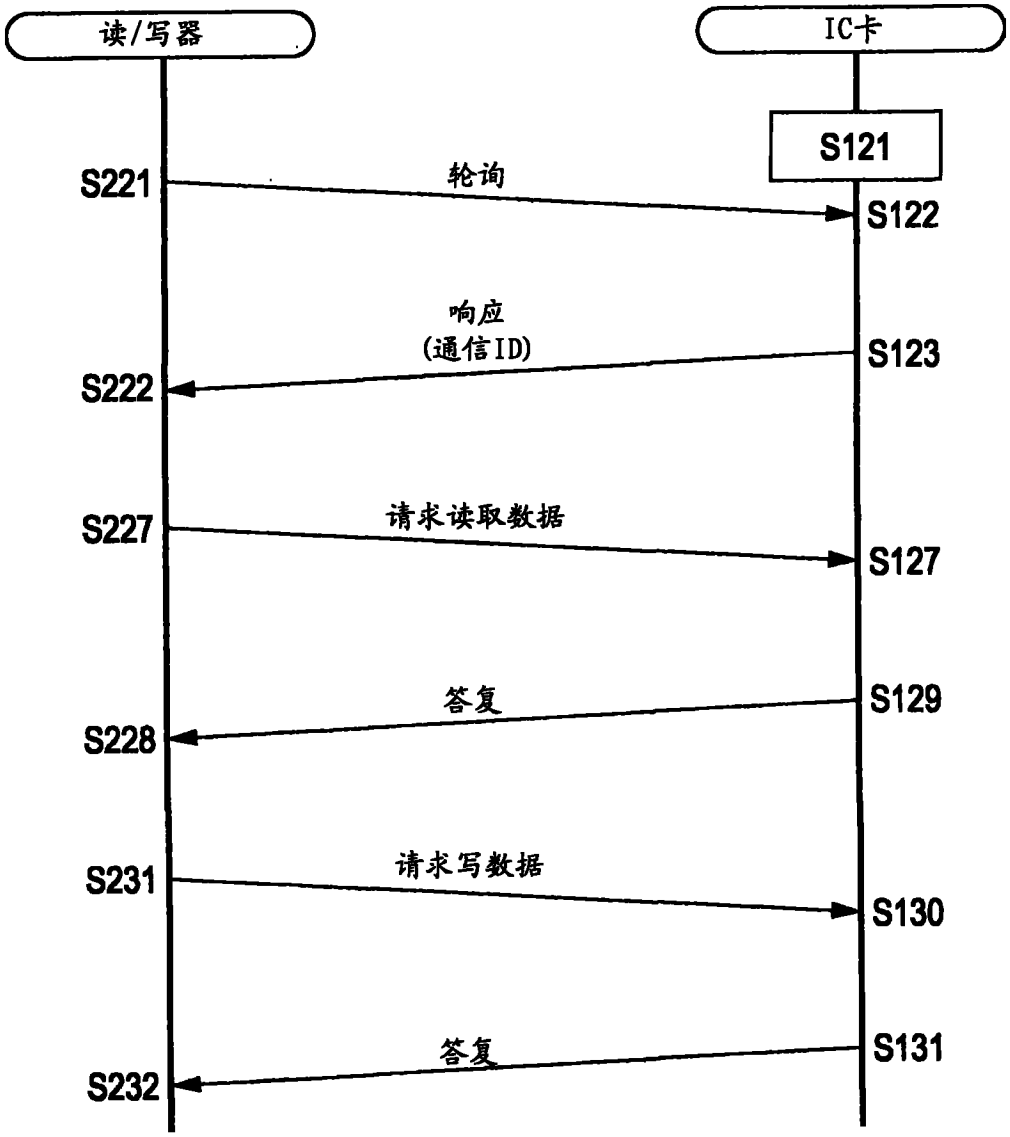

读/写器
IC卡
S121
S221
轮询
S122
响应
(通信ID)
S123
S222
S227
请求读取数据
S127
答复
S129
S228
S231
请求写数据
S130
答复
S131
S232

图 12

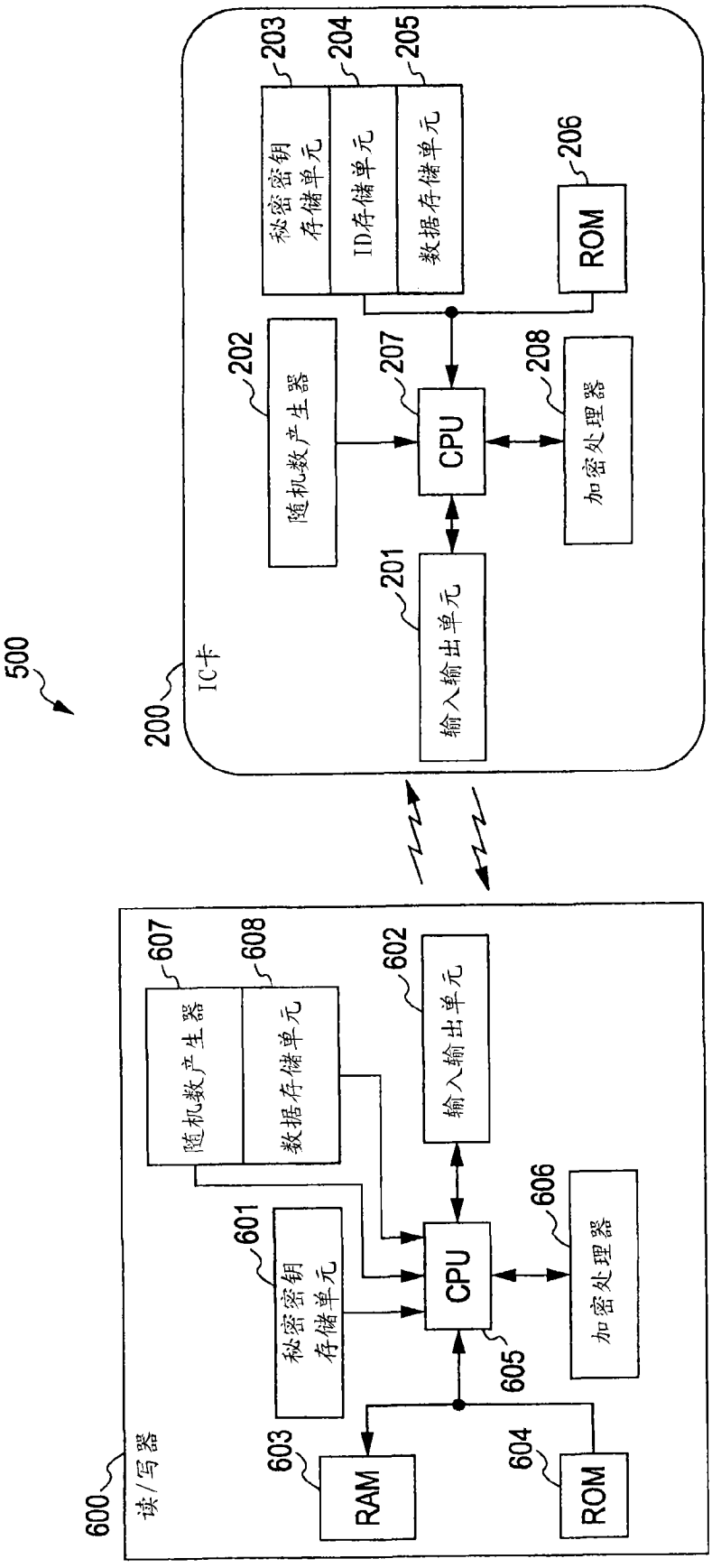

500
200
IC卡
203
秘密密钥存储单元
204
ID存储单元
205
数据存储单元
206
ROM
202
随机数产生器
207
CPU
208
加密处理器
201
输入输出单元
600
读/写器
607
随机数产生器
608
数据存储单元
602
输入输出单元
601
秘密密钥存储单元
606
加密处理器
605
CPU
603
RAM
604
ROM

图 13

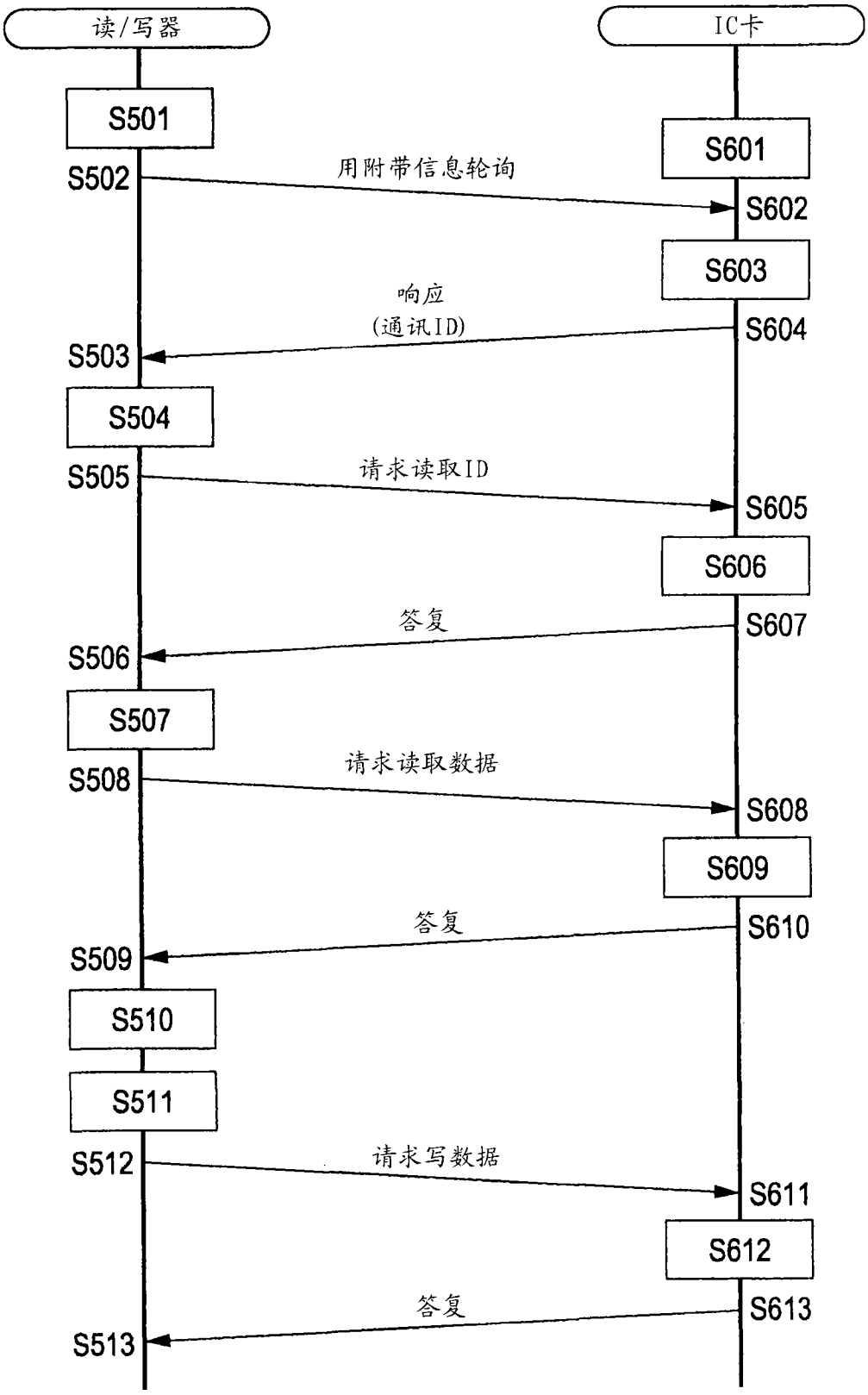

读/写器
IC卡
S501
S601
S502
用附带信息轮询
S602
S603
响应
(通讯ID)
S503
S604
S504
S505
请求读取ID
S605
S606
答复
S506
S607
S507
S508
请求读取数据
S608
S609
答复
S509
S610
S510
S511
S512
请求写数据
S611
S612
答复
S513
S613

图 14

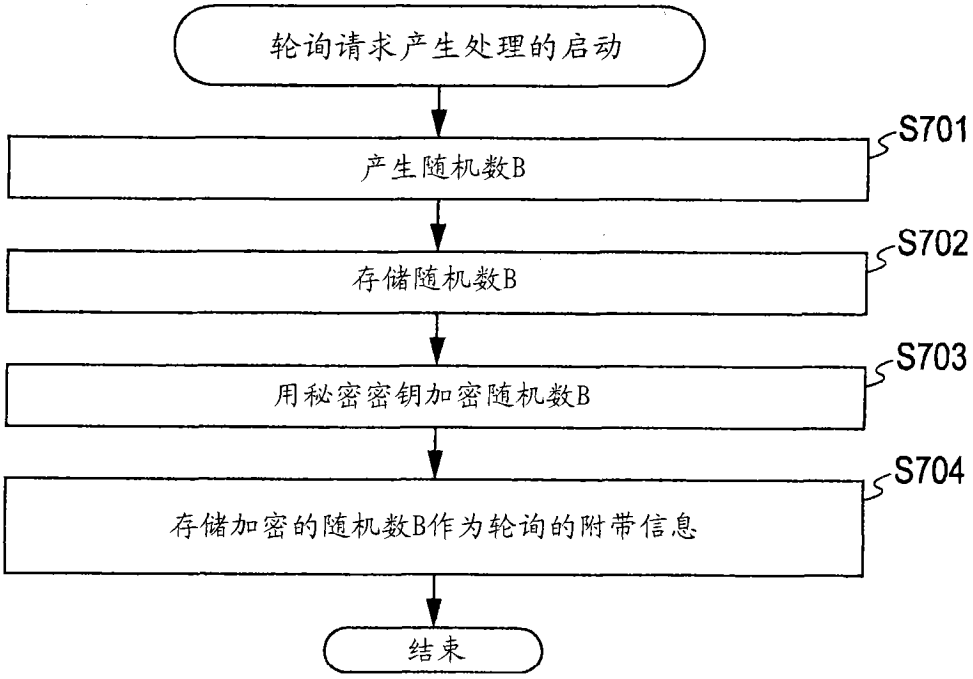

轮询请求产生处理的启动
S701
产生随机数B
S702
存储随机数B
S703
用秘密密钥加密随机数B
S704
存储加密的随机数B作为轮询的附带信息
结束

图 15

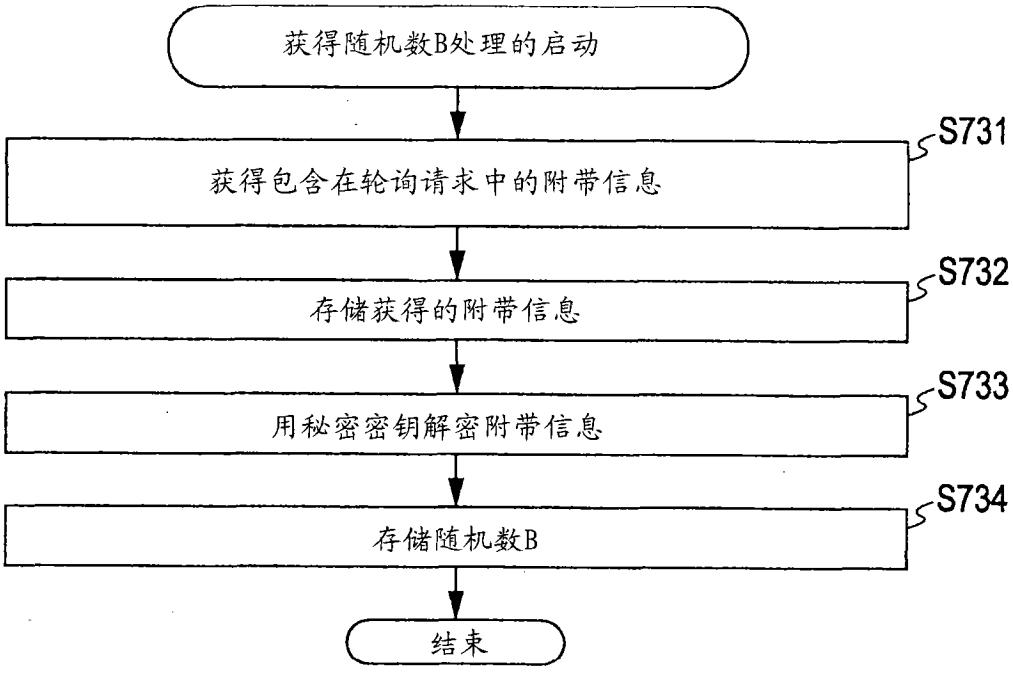

获得随机数B处理的启动
S731
获得包含在轮询请求中的附带信息
S732
存储获得的附带信息
S733
用秘密密钥解密附带信息
S734
存储随机数B
结束

图 16

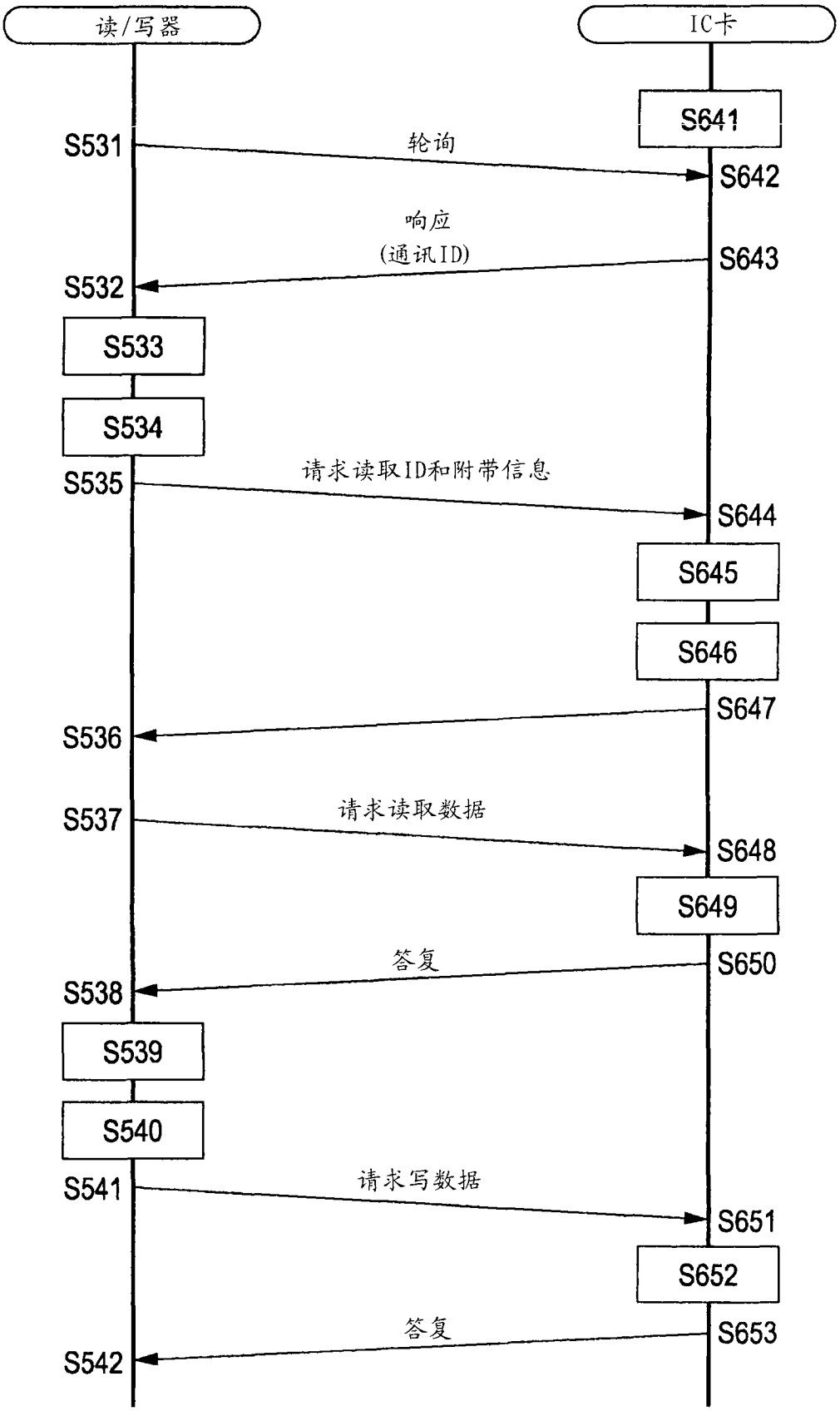

读/写器
IC卡
S641
S531
轮询
S642
响应
(通讯ID)
S643
S532
S533
S534
S535
请求读取ID和附带信息
S644
S645
S646
S647
S536
S537
请求读取数据
S648
S649
答复
S650
S538
S539
S540
S541
请求写数据
S651
S652
答复
S653
S542

图 17

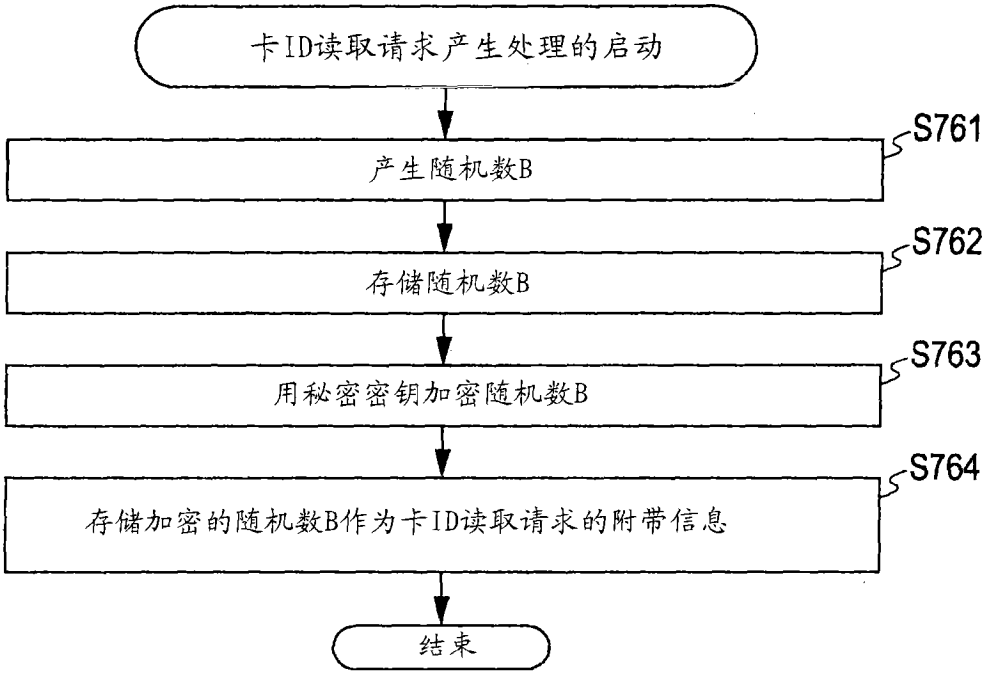

卡ID读取请求产生处理的启动
S761
产生随机数B
S762
存储随机数B
S763
用秘密密钥加密随机数B
S764
存储加密的随机数B作为卡ID读取请求的附带信息
结束

图 18

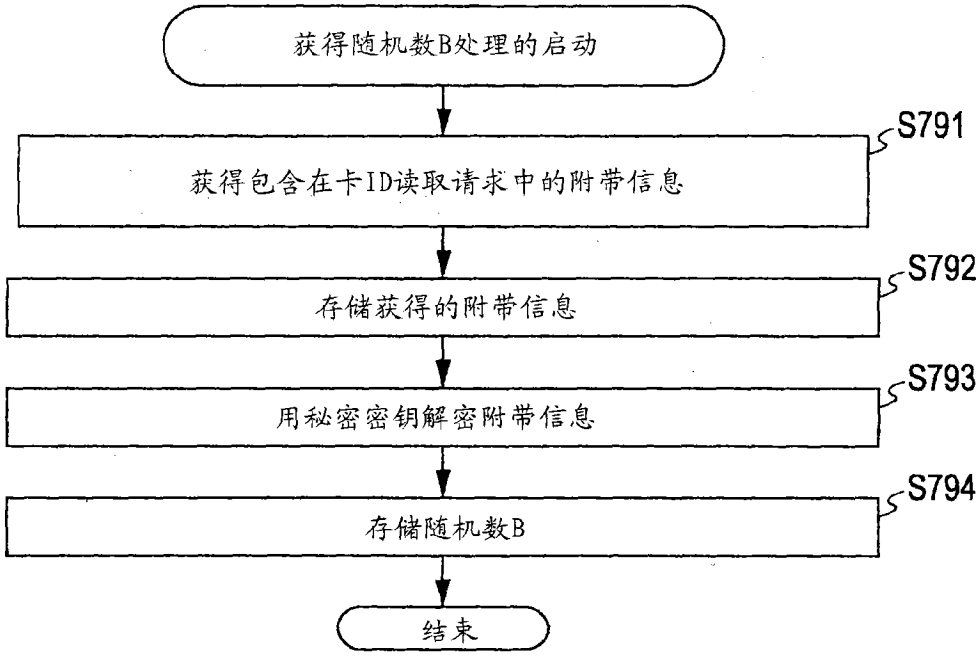

获得随机数B处理的启动
S791
获得包含在卡ID读取请求中的附带信息
S792
存储获得的附带信息
S793
用秘密密钥解密附带信息
S794
存储随机数B
结束

图 19