(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 102333305 B
(45)授权公告日 2015.10.28

(21)申请号 201110148712.4
(22)申请日 2011.06.03
(30)优先权数据
2010-133180 2010.06.10 JP
(73)专利权人 索尼公司
地址 日本东京都
(72)发明人 根岸正树 赤井田彻郎
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 郭定辉
(51)Int.Cl.
H04W 12/00(2009.01)
(56)对比文件
CN 101351987 A ,2009.01.21,
CN 101582125 A ,2009.11.18,
CN 1741029 A ,2006.03.01,
US 6842106 B2 ,2005.01.11,
审查员 王聪

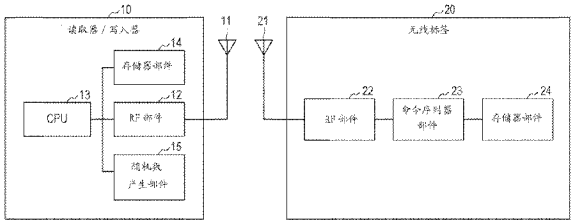
权利要求书5页 说明书19页 附图9页

(54)发明名称

通信设备、通信方法和通信系统

(57)摘要

提供了通信设备、通信方法和通信系统。该通信设备包括：通信部件，进行与读取器/写入器的邻近通信；存储部件，存储数据和序列号；以及控制部件，根据来自读取器/写入器的命令控制数据向存储部件的写入。通信部件将序列号发送到读取器/写入器，并从读取器/写入器接收第一加密数据和作为被写入到存储部件中的目标数据的写目标数据，第一加密数据由读取器/写入器使用基于序列号的值和写目标数据产生，以及控制部件使用基于序列号的所述值和写目标数据产生第二加密数据，在所述第一加密数据和所述第二加密数据相匹配的情况下，将写目标数据写入到存储部件中，并更新序列号。



CN 102333305 B

1. 一种通信设备，包括：

通信装置，进行与读取器 / 写入器的邻近通信；

存储装置，存储数据和序列号，每次数据被写入所述存储装置时，该序列号的值被规律地更新；以及

控制装置，根据来自所述读取器 / 写入器的命令控制数据向所述存储装置的写入，

其中，所述通信装置将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并从所述读取器 / 写入器接收第一加密数据和作为被写入到所述存储装置中的目标数据的写目标数据，所述第一加密数据由所述读取器 / 写入器使用基于所述序列号的值和所述写目标数据产生，以及

所述控制装置使用所述基于序列号的值和由所述通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

2. 根据权利要求 1 的通信设备，

其中，所述基于序列号的值是序列号本身或者更新后的序列号。

3. 根据权利要求 1 的通信设备，

其中，所述读取器 / 写入器产生随机数并将所述随机数发送到所述通信设备，

所述通信装置接收从所述读取器 / 写入器发送的随机数，

所述控制装置使用通过使用区分所述通信设备的区分信息产生的对所述通信设备唯一的单独密钥和由所述通信装置接收的随机数来产生在与所述读取器 / 写入器的会话中使用的会话密钥，并使用所述区分信息和所述会话密钥产生第三加密数据，

所述通信装置将所述区分信息和所述第三加密数据发送到所述读取器 / 写入器，以及

所述读取器 / 写入器使用从所述通信装置发送的区分信息产生所述单独密钥，使用所述单独密钥和所述随机数产生所述会话密钥，使用从所述通信装置发送的区分信息和所述会话密钥产生第四加密数据，通过比较所述第三加密数据和所述第四加密数据来进行验证所述通信设备的单侧验证，并在所述单侧验证成功的情况下将所述第一加密数据和所述写目标数据发送到所述通信设备。

4. 根据权利要求 1 的通信设备，

其中，在所述存储装置中仅提供一个序列号。

5. 根据权利要求 1 的通信设备，

其中，所述存储装置的存储区的一部分是作为能够被分配给服务的最小单元的存储区的用户块，

所述用户块具有多个单元，

所述单元具有作为其中进行写入的预定单元的存储区的页的一页或多页，

配置所述用户块的所述多个单元中的一个单元是起着缓冲被写入到用户块中的数据的缓冲器的作用的缓冲单元，

所述存储装置存储用于管理所述存储装置的存储区的管理信息，

所述管理信息包括指定单元的单元号，以及

所述控制装置通过写入目标单元的单元号作为所述缓冲单元的单元号来进行数据向所述目标单元的写入并将所述目标单元设置为新的缓冲单元，所述目标单元是作为数据要

被写入的目标的单元。

6. 根据权利要求 5 的通信设备，

其中，所述单元被配置为具有一页，

所述存储装置的存储区的另一部分是存储每个用户块的管理信息的管理块，

所述用户块的管理信息包括所述用户块的所述多个单元中每一个的单元号和一个序列号，以及

所述控制装置更新被包括在具有其中写目标数据被写入到的单元的用户块的管理信息中所包括的一个序列号。

7. 根据权利要求 5 的通信设备，

其中，所述单元由多页配置，

一个单元的多页中的一页是存储每个单元的管理信息的管理页，

单元的管理信息包括所述单元的单元号和一个序列号，以及

所述控制装置更新在其中写目标数据被写入到的单元的管理信息中所包括的一个序列号。

8. 根据权利要求 5 的通信设备，

其中，使用所述基于序列号的值、写目标数据和目标单元的单元号来产生所述第一加密数据和所述第二加密数据。

9. 一种通信设备的通信方法，所述通信设备提供有 ：通信装置，进行与读取器 / 写入器的邻近通信 ；存储装置，存储数据和序列号，每次数据被写入所述存储装置时，该序列号的值被规律地更新 ；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向所述存储装置中的写入，所述方法包括步骤 ：

使用所述通信装置将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并从所述读取器 / 写入器接收第一加密数据和作为被写入到所述存储装置中的目标数据的写目标数据，所述第一加密数据由所述读取器 / 写入器使用基于序列号的值和所述写目标数据产生，以及

使用所述控制装置，使用所述基于序列号的值和由所述通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

10. 一种通信设备，包括 ：

通信装置，进行与无线标签的邻近通信，所述无线标签具有存储数据和序列号的存储装置，每次数据被写入所述存储装置中时，该序列号的值被规律地更新 ；以及

产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，

其中，所述通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签，并且

其中，所述无线标签使用所述基于序列号的值和来自所述通信装置的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将所述写目标数据写入到所述存储装置中，并更新存储在所述存储装置中的序列号。

11. 根据权利要求 10 的通信设备，

其中，所述基于序列号的值是序列号本身或者更新后的序列号。

12. 根据权利要求 10 的通信设备，还包括 ：

随机数产生装置，产生所述通信设备使用来验证所述无线标签的随机数，

所述通信装置将所述随机数发送到所述无线标签，

所述无线标签接收从所述通信装置发送的随机数，使用通过使用区分所述无线标签的区分信息产生的、对所述无线标签唯一的单独密钥和所述随机数来产生在与所述通信设备的会话中使用的会话密钥，使用所述区分信息和所述会话密钥产生第三加密数据，并将所述区分信息和所述第三加密数据发送到所述通信设备，

所述产生装置使用从所述无线标签发送的区分信息产生所述单独密钥，使用所述单独密钥和所述随机数产生所述会话密钥，使用从所述无线标签发送的区分信息和所述会话密钥产生第四加密数据，并通过比较所述第三加密数据和所述第四加密数据来进行验证所述无线标签的单侧验证，以及

在所述单侧验证成功的情况下，所述通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签。

13. 一种通信设备的通信方法，所述通信设备提供有 ：通信装置，进行与无线标签的邻近通信，所述无线标签具有存储数据和序列号的存储装置，每次数据被写入所述存储装置中时，该序列号的值被规律地更新 ；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，所述方法包括步骤 ：

使用所述产生装置产生所述第一加密数据 ；以及

使用所述通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签，

其中，所述无线标签使用所述基于序列号的值和来自所述通信装置的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将所述写目标数据写入到所述存储装置中，并更新存储在所述存储装置中的序列号。

14. 一种通信系统，包括 ：

读取器 / 写入器和无线标签，进行邻近通信，

其中，所述读取器 / 写入器具有 ：第一通信装置，进行与所述无线标签的邻近通信，所述无线标签具有存储数据和序列号的存储装置，每次数据被写入所述存储装置中时，该序列号的值被规律地更新 ；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，

所述第一通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签，

所述无线标签具有 ：第二通信装置，进行与所述读取器 / 写入器的邻近通信 ；存储装置 ；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向所述存储装置的写入，

所述第二通信装置将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并接收从所述读取器 / 写入器发送的第一加密数据和写目标数据，以及

所述控制装置使用所述基于序列号的值和由所述第二通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述第二通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序

列号。

15. 一种通信系统的通信方法，所述通信系统提供有进行邻近通信的读取器 / 写入器和无线标签，其中，所述读取器 / 写入器具有 ：第一通信装置，进行与所述无线标签的邻近通信，所述无线标签具有存储数据和序列号的存储装置，每次数据被写入所述存储装置中时，该序列号的值被规律地更新 ；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，以及所述无线标签具有 ：第二通信装置，进行与所述读取器 / 写入器的邻近通信 ；存储装置 ；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向所述存储装置的写入，所述方法包括步骤 ：

使用所述第一通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签 ；

使用所述第二通信装置，将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并接收从所述读取器 / 写入器发送的第一加密数据和写目标数据 ；

使用所述基于序列号的值和由所述第二通信装置接收的写目标数据产生第二加密数据 ；以及

在所述第一加密数据和所述第二加密数据相匹配的情况下，使用所述控制装置，将由所述第二通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

16. 一种通信设备，包括 ：

通信部件，进行与读取器 / 写入器的邻近通信 ；

存储部件，存储数据和序列号，每次数据被写入所述存储部件中时，该序列号的值被规律地更新 ；以及

控制部件，根据来自所述读取器 / 写入器的命令控制数据向所述存储部件的写入，

其中，所述通信部件将存储在所述存储部件中的序列号发送到所述读取器 / 写入器，并从所述读取器 / 写入器接收第一加密数据和作为被写入到所述存储部件中的目标数据的写目标数据，所述第一加密数据由所述读取器 / 写入器使用基于序列号的值和所述写目标数据产生，以及

所述控制部件使用所述基于序列号的值和由所述通信部分接收的写目标数据产生第二加密数据，在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信部件接收的写目标数据写入到所述存储部件中，并更新所述存储部件中存储的序列号。

17. 一种通信设备，包括 ：

通信部件，进行与无线标签的邻近通信，所述无线标签具有存储数据和序列号的存储部件，每次数据被写入所述存储部件中时，该序列号的值被规律地更新 ；以及

产生部件，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储部件中的目标数据的写目标数据产生第一加密数据，

其中，所述通信部件将所述第一加密数据和所述写目标数据发送到所述无线标签，并且

其中，所述无线标签使用所述基于序列号的值和来自所述通信装置的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将所述写目

标数据写入到所述存储装置中，并更新存储在所述存储装置中的序列号。

通信设备、通信方法和通信系统

技术领域

[0001] 本发明涉及通信设备、通信方法和通信系统，具体地，涉及通信设备、通信方法和通信系统，其能够实现无线标签的尺寸减小以及成本降低，同时确保关于进行例如与读取器 / 写入器的邻近通信的诸如 IC 卡或 IC 芯片之类的无线标签的安全性。

背景技术

[0002] 近年来，使用 IC（集成电路）卡等在近距离不接触地进行无线通信的邻近通信用于例如电子通勤月票、电子货币等，并且具有使用邻近通信的电子通行月票或电子货币功能的移动电话设备也广泛使用。

[0003] 邻近通信已经被标准化为例如 ISO/IEC 14443 和 ISO/IEC 18092 中（下文中称为 NFC（近场通信））。

[0004] 在此，在进行诸如基于 NFC 标准的通信之类的邻近通信的通信设备中，以响应于来自读取器 / 写入器的信号的格式与输出 RF（射频）信号的读取器 / 写入器进行邻近通信的诸如 IC 卡或 IC 芯片之类的通信设备被称为无线标签。

[0005] 例如，该无线标签通过内置诸如 EEPROM（电可擦除可编程只读存储器）之类的非易失性存储器、并在该非易失性存储器中进行读取和写入使用邻近通信与读取器 / 写入器交换的数据来提供各种类型的服务。

[0006] 在读取器 / 写入器和无线标签中，为了防止由与欺骗性设备 (fraudulent device) 进行的邻近通信篡改在内置于无线标签中的非易失性存储器中所存储的数据，例如根据对称密码算法进行相互验证（例如，日本未审查专利申请公开 No. 2009-276916）。

[0007] 在根据对称密码算法的相互验证中，读取器 / 写入器和无线标签中的一个、例如读取器 / 写入器产生随机数 RA，并通过使用公钥 KA 加密该随机数 RA，产生随机数 RA 的加密数据 $\{RA\}_{KA}$，并将其发送到无线标签。

[0008] 无线标签从读取器 / 写入器接收该加密数据 $\{RA\}_{KA}$ 并使用公钥 KA 解密该加密数据 $\{RA\}_{KA}$。此外，通过使用公钥 KB 加密该加密数据 $\{RA\}_{KA}$ 的解密结果 RA’，产生解密结果 RA’ 的加密数据 $\{RA'\}_{KB}$，并通过无线标签将其发送到读取器 / 写入器。

[0009] 读取器 / 写入器从无线标签接收该加密数据 $\{RA'\}_{KB}$ 并使用公钥 KB 解密该加密数据 $\{RA'\}_{KB}$。然后，读取器 / 写入器通过将加密数据 $\{RA'\}_{KB}$ 的解密结果 RA” 与随机数 RA 相比较来进行无线标签是否是合法设备 (legitimate device) 的验证。

[0010] 即，在加密数据 $\{RA'\}_{KB}$ 的解密结果 RA” 与随机数 RA 相互匹配的情况下，因为无线标签具有公钥 KA 和 KB，因此读取器 / 写入器识别出该无线标签是合法设备（无线标签的验证成功）。

[0011] 另外，在根据对称密码算法的相互验证中，读取器 / 写入器和无线标签中的另一个、例如无线标签产生随机数 RB，并通过进行与读取器 / 写入器验证无线标签的以下情况相同的方式进行处理，所述无线标签进行读取器 / 写入器是否是合法设备的验证。

[0012] 然后，当读取器 / 写入器的验证在无线标签中成功时，在读取器 / 写入器和无线标

签中，使用随机数 RA 和 RB 产生加密密钥，并使用该加密密钥对数据加密，并且进行数据交换。

[0013] 从而，在相互验证已经成功的读取器 / 写入器和无线标签之间，因为交换通过使用加密密钥对数据加密而获得的加密数据，能够防止数据的窃听。

发明内容

[0014] 如以上，在根据对称密码算法在读取器 / 写入器和无线标签之间进行相互验证的情况下，在读取器 / 写入器和无线标签两者中，产生随机数的电路（随机数产生电路）是必须的。

[0015] 但是，在无线标签中提供随机数产生电路妨碍了无线标签的尺寸减小和成本降低。

[0016] 另一方面，在无线标签中不提供随机数产生电路的情况下，不能根据对称密码算法在相互验证中从无线标签进行读取器 / 写入器是否是合法设备的验证。

[0017] 在此，关于无线标签，对于用在诸如对在给定的一天或短时段、比如几天内举行的诸如音乐会之类的事件的票证的服务中，存在增加的预期。

[0018] 关于不同于诸如在主题公园等处多次通行 (multi-pass) 的事件的票证的、有效时段（可以使用票证或多次通行的时段）限于短时段的服务（以下称为短期服务），即使自从使用欺骗性无线标签起进行了合法无线标签的分析，因为在分析完成之前有效时段已经过去，不需要具有像诸如电子货币等没有有效时段的服务所要求的那样强的安全性。

[0019] 如以上，关于用于短期服务的无线标签，不需要具有像没有有效时段的服务所要求的那样强的安全性，但即使这样，也需要将安全性确保到在短期服务的有效时段中难以进行无线标签的分析的程度。

[0020] 期望能够实现无线标签的尺寸减小和成本降低同时确保关于无线标签的安全性。

[0021] 根据本发明第一实施例的通信设备提供有：通信装置，进行与读取器 / 写入器的邻近通信；存储装置，存储数据和序列号，每次数据被写入到存储装置中时，该序列号的值被规律地更新；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向存储装置中的写入；其中所述通信装置将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并从所述读取器 / 写入器接收第一加密数据和作为被写入到所述存储装置中的目标数据的写目标数据，该第一加密数据由读取器 / 写入器使用基于所述序列号的值和所述写目标数据而产生；以及所述控制装置使用基于所述序列号的值和由所述通信装置接收的写目标数据产生第二加密数据，在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0022] 根据本发明第一实施例的通信设备的通信方法，所述通信设备提供有：通信装置，进行与读取器 / 写入器的邻近通信；存储装置，存储数据和序列号，每次数据被写入到存储装置中时，该序列号的值被规律地更新；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向存储装置中的写入，所述方法包括步骤：将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并从所述读取器 / 写入器接收第一加密数据和作为被写入到所述存储装置中的目标数据的写目标数据，该第一加密数据由读取器 / 写入器使用基于所

述序列号的值和所述写目标数据而产生，以及使用基于所述序列号的值和由所述通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0023] 在本发明的第一实施例中，通信装置将存储在存储装置中的序列号发送到读取器/写入器，并从读取器/写入器接收第一加密数据和作为被写入到存储装置中的目标数据的写目标数据，所述第一加密数据由所述读取器/写入器使用基于序列号的值和所述写目标数据产生。然后，控制装置使用基于所述序列号的值和由所述通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0024] 根据本发明第二实施例的通信设备提供有：通信装置，进行与无线标签的邻近通信，该无线标签具有存储数据和序列号的存储装置，每次数据写入到存储部件中时，该序列号的值被规律地更新；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据；其中所述通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签。

[0025] 根据本发明第二实施例的通信设备的通信方法，所述通信设备提供有：通信装置，进行与无线标签的邻近通信，该无线标签具有存储数据和序列号的存储装置，每次数据写入到存储装置中时，该序列号的值被规律地更新；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，所述方法包括步骤：产生所述第一加密数据；以及将所述第一加密数据和所述写目标数据发送到所述无线标签。

[0026] 在本发明的第二实施例中，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，并且第一加密数据和写目标数据被发送到无线标签。

[0027] 根据本发明第三实施例的通信系统提供有：进行邻近通信的读取器/写入器和无线标签；其中，所述读取器/写入器具有：第一通信装置，进行与所述无线标签的邻近通信，该无线标签具有存储数据和序列号的存储装置，每次数据被写入到存储装置中时，该序列号的值被规律地更新；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，其中所述第一通信装置将所述第一加密数据和所述写目标数据发送到所述无线标签；以及所述无线标签具有：第二通信装置，进行与所述读取器/写入器的邻近通信；存储装置；以及控制装置，根据来自所述读取器/写入器的命令控制数据向存储装置的写入，其中所述第二通信装置将存储在所述存储装置中的序列号发送到所述读取器/写入器，并接收从所述读取器/写入器发送的第一加密数据和写目标数据，以及所述控制装置使用基于所述序列号的值和由所述第二通信装置接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述第二通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0028] 根据本发明第三实施例的通信系统的通信方法，该通信系统提供有进行邻近通信

的读取器 / 写入器和无线标签，其中所述读取器 / 写入器具有 ：第一通信装置，进行与所述无线标签的邻近通信，该无线标签具有存储数据和序列号的存储装置，每次数据被写入到存储装置中时，该序列号的值被规律地更新 ；以及产生装置，使用基于从所述无线标签发送的序列号的值和作为被写入到所述存储装置中的目标数据的写目标数据产生第一加密数据，以及所述无线标签具有 ：第二通信装置，进行与所述读取器 / 写入器的邻近通信 ；存储装置 ；以及控制装置，根据来自所述读取器 / 写入器的命令控制数据向存储装置的写入，所述方法包括步骤 ：将所述第一加密数据和所述写目标数据发送到所述无线标签 ；将存储在所述存储装置中的序列号发送到所述读取器 / 写入器，并接收从所述读取器 / 写入器发送的第一加密数据和写目标数据 ；使用基于所述序列号的值和由所述第二通信装置接收的写目标数据产生第二加密数据 ；以及在所述第一加密数据和所述第二加密数据相匹配的情况下，将由所述第二通信装置接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0029] 在本发明的第三实施例中，无线标签将存储在存储装置中的序列号发送到读取器 / 写入器，并且接收第一加密数据和写目标数据，该第一加密数据由读取器 / 写入器使用基于该序列号的值和写目标数据产生。此外，无线标签使用所述序列号的值和所接收的写目标数据产生第二加密数据，并在所述第一加密数据和所述第二加密数据相匹配的情况下，将所接收的写目标数据写入到所述存储装置中，并更新所述存储装置中存储的序列号。

[0030] 在此，该通信设备可以是独立的设备或者可以是配置一个设备的内部块。

[0031] 根据本发明的第一到第三实施例，关于作为进行与读取器 / 写入器的邻近通信的通信设备的无线标签，能够实现无线标签的尺寸减小以及成本降低同时确保安全性。

附图说明

[0032] 图 1 是图示根据本发明实施例的通信系统的配置示例的框图 ；

[0033] 图 2 是图示存储器部件的逻辑格式的示例的示图 ；

[0034] 图 3 是描述到存储器部件的数据写入的示图 ；

[0035] 图 4 是描述针对存储器讹误的手段的示图 ；

[0036] 图 5 是图示存储在读取器 / 写入器的存储器部件和无线标签的存储器部件中的单侧验证所需的信息的示图 ；

[0037] 图 6 是描述在读取器 / 写入器进行单侧验证的情况下读取器 / 写入器和无线标签的处理的示图 ；

[0038] 图 7 是描述在读取器 / 写入器进行单侧验证并且无线标签使用单侧验证进行读取器 / 写入器的验证的情况下读取器 / 写入器和无线标签的处理的示图 ；

[0039] 图 8 是描述在读取器 / 写入器进行单侧验证并且无线标签使用单侧验证进行读取器 / 写入器的验证的情况下读取器 / 写入器和无线标签的处理的示图 ；以及

[0040] 图 9 是图示存储器部件的逻辑格式的另一示例的示图。

具体实施方式

[0041] 根据本发明实施例的通信系统

[0042] 图 1 是图示根据本发明实施例的通信系统（系统指多个设备的逻辑集合，无论每

个构成设备是否处于相同的外壳中）的配置示例的框图。

[0043] 在图 1 中，由读取器 / 写入器 10 和无线标签 20 构成通信系统。

[0044] 读取器 / 写入器 10 通过从天线 11 输出 RF 信号不接触地进行与无线标签 20 的邻近通信，数据被存储（写入）在无线标签 20（中内置的存储器部件 24）中，或者从无线标签 20 读出数据。

[0045] 即，读取器 / 写入器 10 具有天线 11、RF 部件 12、CPU（中央处理单元）13、存储器部件 14 和随机数产生部件 15。

[0046] 天线 11 通过例如由线圈和电容器 (condenser) 形成的谐振电路构成，并发送来自 RF 部件 12 的 RF 信号。

[0047] RF 部件 12 进行与无线标签 20 的邻近通信。

[0048] 即，通过从天线 11 输出通过根据来自 CPU 13 的命令和数据对作为 RF 信号的载波的调制而获得的调制信号，RF 部件 12 将命令和数据发送到无线标签 20。

[0049] 另外，RF 部件 12 从天线 11 输出作为 RF 信号的载波，并且无线标签接收通过对作为 RF 信号的载波的负载调制而发送的数据等。

[0050] CPU 13 通过执行在存储器部件 14 中存储的程序来进行构成读取器 / 写入器 10 的每个块的控制和其他处理。

[0051] 存储器部件 14 存储由 CPU 13 执行的程序。另外，存储器部件 14 存储从无线标签 20 读出的数据、写入到无线标签 20 中的数据等。

[0052] 随机数产生部件 15 产生在单侧验证中使用的随机数，在该单侧验证中，存在（读取器 / 写入器 10 的）无线标签 20 是否是合法设备的验证。

[0053] 当使得无线标签 20 接近读取器 / 写入器 10 时，无线标签 20 开始以读取器 / 写入器 10 从天线 11 输出的 RF 信号作为电源来操作，并进行与读取器 / 写入器 10 的邻近通信。

[0054] 在邻近通信中，读取器 / 写入器 10 通过根据数据对 RF 信号的调制来发送数据，并且无线标签 20 接收读取器 / 写入器 10 使用 RF 信号发送的数据，并将该数据写入到内置的存储器部件中 24。

[0055] 另外，无线标签 20 读出存储器部件 24 中存储的数据，并通过对从读取器 / 写入器 10 发送的 RF 信号的负载调制将数据发送到读取器 / 写入器 10。

[0056] 即，无线标签 20 具有天线 21、RF 部件 22、命令序列器部件 23 和存储器部件 24。

[0057] 天线 21 通过例如由线圈和电容器形成的谐振电路配置，接收来自读取器 / 写入器 10 的 RF 信号，并将该 RF 信号提供给 RF 部件 22。

[0058] RF 部件 22 进行与读取器 / 写入器 10 的邻近通信。

[0059] 即，当使用天线 21 接收来自读取器 / 写入器 10 的 RF 信号时，由于使得读取器 / 写入器 10 和无线标签 20 接近，RF 部件 22 从 RF 信号获得作为电源的电力并将该电力提供给所需的块。

[0060] 另外，RF 部件 22 将来自读取器 / 写入器 10 的 RF 信号解调为命令和数据，并将该命令和数据提供给命令序列器部件 23。

[0061] 此外，RF 部件 22 通过根据从命令序列器部件 23 提供的数据对来自读取器 / 写入器 10 的 RF 信号的负载调制将数据发送到读取器 / 写入器 10。

[0062] 命令序列器部件 23 通过根据从 RF 部件 22 提供的来自读取器 / 写入器 10 的命令

进行序列控制来进行诸如对存储器部件 24 数据读和写之类的控制。

[0063] 即，在来自读取器 / 写入器 10 的命令是请求写入数据的写入命令的情况下，命令序列器部件 23 将与该写入命令一起从读取器 / 写入器 10 发送并从 RF 部件 22 提供的数据写入到存储器部件 24 中。

[0064] 另外，在来自读取器 / 写入器 10 的命令是请求读出数据的读取命令的情况下，命令序列器部件 23 从存储器部件 24 读出数据，并将该数据提供给 RF 部件 22。

[0065] 存储器部件 24 是例如诸如 EEPROM 等的非易失性存储器，并在命令序列器部件 23 的控制（管理）下存储数据。

[0066] 在此，如上所述，读取器 / 写入器 10 具有产生在无线标签 20 的验证中使用的随机数的随机数产生部件 15，但是无线标签不具有产生在读取器 / 写入器 10 的验证中使用的随机数的电路。

[0067] 因此，可以减小无线标签 20 的尺寸和降低无线标签 20 的成本到无线标签 20 不具有产生随机数的电路的程度。

[0068] 这里，因为无线标签 20 不具有产生随机数的电路，所以无线标签 20 不能使用随机数来验证读取器 / 写入器 10。

[0069] 但是，在无线标签 20 中，在安全性方面，根本不进行读取器 / 写入器 10 的验证不是优选的。

[0070] 因此，无线标签 20 通过使用稍后将描述的可以称为简化的验证方法进行读取器 / 写入器 10 的验证，来限制从欺骗性读取器 / 写入器的访问，并且据此，确保了比最低需要更大的安全性。

[0071] 存储器部件 24 的逻辑格式

[0072] 图 2 是描述图 1 的无线标签 20 的存储器部件 24 的逻辑格式的示图。

[0073] 存储器部件 24 的一部分存储区是作为能够分配给例如通勤月票、由某些服务提供者管理的电子货币或者诸如对一事件的计票 (ticketing) 之类的服务等的最小单元的存储区的用户块。

[0074] 在存储器部件 24 中，提供一个或多个用户块。

[0075] 在此，为服务分配一个或多个用户块，并且用于提供服务的数据存储在一个或多个用户块中。

[0076] 用户块具有数量是作为复数的 M+1 的单元 (M 是 1 或更大的整数)。

[0077] 用于提供服务的数据被写入到各单元中。但是，配置用户块的 M+1 个单元中的一个单元起着缓冲被写入到用户块中的数据的缓冲器的作用。

[0078] 如上所述，因为配置用户块的一个单元起着缓冲器的作用，因此用户块具有数量是作为复数的 M+1 的单元，这是起着缓冲器作用的一个单元和存储用于提供服务的数据的一个或更多的 M 个单元的总数。

[0079] 在此，在配置用户块的 M+1 个单元中的起着缓冲器的作用的单元以下被称为缓冲单元，并且不是缓冲单元的单元是数据单元。

[0080] 在图 2 中，配置用户块的 M+1 个单元中的第 M+1 个单元是缓冲单元，并且第一到第 M 个单元是数据单元。

[0081] 在此，当进行在用户块中的数据写入时，作为缓冲单元的单元改变，但是稍后将描

述对其的描述。

[0082] 该单元具有数量是 1 或更大的 K 个页。

[0083] 页是能够对存储器部件 24 进行写入的最小单元的存储区，在图 2 中，一页是具有 N 位的存储区。

[0084] 在此，在图 2 中，单元的各页中的一页用作存储用于管理存储器部件 24 的存储区的管理信息的页（管理页）。

[0085] 即，在图 2 中，配置该单元的 K 个页中的一个预定页是其中存储了用于管理该单元的管理信息的管理页。

[0086] 从而，在图 2 中，因为存储数据的一页或多页（数据页）和一个管理页是单元中所需的，配置该单元的页的数量 K 是复数。

[0087] 在此，在图 2 中，配置该单元的 K 页中的第 K 页是管理页。作为管理页的页不改变（类似于缓冲单元）并且是固定页。

[0088] 单元号、（一个）序列号和误差检测码被写入到管理页中作为单元管理信息。

[0089] 单元号是指定具有其中写入了单元号的管理页的单元的信息。

[0090] 序列号是每次数据被写入到存储器部件 24 中时规律地更新的值，并且例如，能够采用使用一表格以先前值作为输入值而确定的输出值等，在该表格中，存在相对于先前值递增或递减诸如 1 的预定值的值、以先前值作为参数通过计算预定函数而确定的值、输入值和输出值之间的链接。

[0091] 另外，在此，例如每次数据被写入到存储器部件 24 中时递增 1 的值被设置为用作序列号。

[0092] 误差检测码是用于检测被写入到单元中的数据中的误差的误差检测的代码，并且例如是 CRC（循环冗余校验）等。

[0093] 数据向存储器部件 24 的写入的控制

[0094] 图 3 是描述使用命令序列器部件 23 对数据向存储器部件 24 的写入的控制的图。

[0095] 在图 3 中，具有其中写入数据的单元的用户块具有 M+1 个单元 #1、#2、.....、#M+1。

[0096] 然后，在图 3 中，在进行数据写入之前（在写入之前），例如，单元 #1 到 #M+1 中的第 M+1 个单元 #M+1 是缓冲单元，并且其它的第 1 到第 M 个单元 #1 到 #M 是数据单元。

[0097] 另外，在图 3 中，在写入之前数据单元 #m 的单元号 S_PAD 是值 m。

[0098] 在此，不向缓冲单元给出单元号 S_PAD，但是在图 3 中（以及在稍后描述的图 5 中以类似方式），为了方便，作为缓冲单元的单元 #M+1 的单元号 S_PAD 被设置为 0，作为指示缓冲单元的值。

[0099] 另外，在图 3 中，在写入之前数据单元 #1 的单元号 SEQ 是值 X。省略了其它数据单元 #2 到 #M 的序列号 SEQ 的图示表示。

[0100] 在此，一个单元 #m 由 K 页配置。在此，第一单元块的单元 #1 的第一页被设置为第一页，并且单元 #m 由第 (m-1)K+1 页到第 mK 页的 K 页配置。然后，作为每个单元 #m 的最后页的第 mK 页是管理页。

[0101] 在此，例如，关于读取器 / 写入器 10 和无线标签 20，请求到其中单元号 S_PAD 具有值 1 的单元的数据写入的写入命令被设置为与数据一起发送。

[0102] 在此情况下，命令序列器部件 23 根据来自读取器 / 写入器 10 的写命令将与写命令一起发送的数据写入到作为缓冲单元的单元 #M+1，并且不写入到作为要进行写入的目标的单元的目标单元，即不写入到单元号 S_PAD 具有值 1 的单元 #1（具有由写入命令请求写入的单元号 S_PAD 的单元）。

[0103] 此外，命令序列器部件 23 将与作为目标单元的单元 #1 的单元号 S_PAD ＝ 1 相同的单元号 S_PAD ＝ 1、更新为预定值 Y 的序列号 SEQ 以及误差检测码写入到作为缓冲单元的单元 #M+1 的管理页。

[0104] 在此，在图 3 中（以及在稍后所述的图 4 中以类似的方式），省略了误差检测码的图示表示。

[0105] 另外，在图 3 中，被写入到作为缓冲单元的单元 #M+1 的管理页中的具有值 Y 的序列号 SEQ 是通过将被写入到作为目标单元的单元 #1 的管理页中的序列号 SEQ ＝ X 仅递增 1 而更新的值 X+1。

[0106] 如上所述，通过将值是 1 的单元号 S_PAD、更新为预定值 Y 的序列号 SEQ 以及误差检测码写入到作为缓冲单元的单元 #M+1 的管理页中，单元 #M+1 变为单元号 S_PAD 具有值 1 并且不是缓冲单元的数据单元。

[0107] 结果，在此时间点，具有值 1 的单元号 S_PAD 的单元变为单元 #1 和单元 #M+1 两个。

[0108] 在此，单元 #M+1 的序列号 SEQ ＝ Y 变为比单元 #1 的序列号 SEQ ＝ x 更新的值，即序列号 SEQ ＝ X 已经被更新的值 X+1。

[0109] 从而，关于单元号 S_PAD 具有值 1 的单元 #1 和单元 #M+1 这两个单元，能够通过参考序列号 SEQ 在已经写入了最后数据的单元 #M+1 和先前写入数据的单元 #1（存储了被写入到单元号 S_PAD 具有值 1 的单元中的数据中的、紧接在最后数据之前写入的数据的单元）之间进行区分。

[0110] 在此，在存在具有相同单元号 S_PAD 的两个单元的情况下，在这两个单元中，写入了最后数据的单元（在此实施例中具有更大的序列号的单元）被称为新单元，并且在过去写入数据的单元（在此实施例中具有较小的序列号的单元）被称为旧单元。

[0111] 在那之后，命令序列器部件 23 擦除单元号 S_PAD 具有值 1 的单元 #1 和单元 #M+1 这两个中的较旧的单元、即作为目标单元的单元 #1 的管理页，并通过在擦除状态下，完成将数据写入到以单元 #1 作为新缓冲单元的存储器部件 24 中的写入处理。

[0112] 在此，如上所述，不向缓冲单元给出单元号 S_PAD，而是在图 3 中，将作为新缓冲单元的单元 #1 的单元号 S_PAD 设置为指示缓冲单元的值 0。

[0113] 如上所述，命令序列器部件 23 根据来自读取器 / 写入器 10 的写命令将数据写入到作为缓冲单元的单元 #M+1 中，作为目标单元的单元 #1 的单元号 S_PAD ＝ 1 被写入作为缓冲单元的单元号，并且进行向作为单元 #1 被设置为新缓冲单元的结果而作为目标单元的单元号 S_PAD 是值 1 的单元 #M+1 的数据写入。

[0114] 结果，在存储器部件 24 中，关于存储在单元号 S_PAD 是值 1 的单元中的数据，因为最后数据（图 3 中被写入到单元 #M+1 中的数据）被写入，同时紧接在之前的（先前）数据（在图 3 中被写入到单元 #1 中的数据）照原样留下，因此能够应对由于存储器讹误、即例如在进行对存储器部件 24 的访问等期间无线标签 20 与读取器 / 写入器 10 分离引起的存储器部件 24 中存储的数据不一致的情况。

[0115] 图 4 是描述针对存储器讹误的手段的图。

[0116] 在图 4 中，在写入之前，以与图 3 的情况相同的方式，第 M+1 个单元 #M+1 是缓冲单元，并且第一到第 M 单元 #1 到 #M 是数据单元。

[0117] 另外，在写入之前，数据单元 #m 的单元号 S_PAD 是值 m，并且作为缓冲单元的单元 #M+1 的单元号 S_PAD 是指示缓冲单元的值 0。

[0118] 在此，例如，以与图 3 相同的方式，关于从读取器 / 写入器 10 到无线标签 20，请求到作为单元号 S_PAD 具有值 1 的单元的目标单元的数据写入的写入命令被设置为与数据一起发送。

[0119] 在此情况下，如图 3 所述，命令序列器部件 23 根据来自读取器 / 写入器 10 的写入命令将与写入命令一起发送的数据写入到作为缓冲单元的单元 #M+1（单元号 S_PAD 是值 0 的单元）中。

[0120] 此外，如图 3 所述，命令序列器部件 23 将与作为目标单元的单元 #1 的单元号 S_PAD ＝ 1 相同的单元号 S_PAD ＝ 1、其中作为目标单元的单元 #1 的序列号 SEQ 已经被更新的具有值 Y ＝ X+1 的序列号 SEQ 以及误差检测码写入到作为缓冲单元的单元 #M+1 的管理页，并在那之后，擦除作为目标单元的单元 #1 的管理页，且通过在擦除状态下，完成将数据写入到以单元 #1 作为新缓冲单元的存储器部件 24 中的写入处理。

[0121] 在此，在写入处理期间，即例如在单元号 S_PAD ＝ 1、其中预定值 Y 已经被更新的序列号 SEQ 以及误差检测码正被写入到作为缓冲单元的单元 #1 的管理页中期间，无线标签 20 与读取器 / 写入器 10 分离，并且所需的电力未被提供给无线标签 20（电源断开）。

[0122] 在此情况下，接下来，当供应电源并且由于使得读取器 / 写入器 10 和无线标签 20 接近而激活时（下一次激活），命令序列器部件 23 恢复存储器部件 24 的存储内容。

[0123] 即，例如，当在单元号 S_PAD ＝ 1、其中预定值 Y 已经被更新的序列号 SEQ 和误差检测码之中至少单元号 S_PAD ＝ 1 和具有预定值 Y 的序列号 SEQ 被写入到作为缓冲单元的单元 #M+1 的管理页中之后切断电源时，存在单元号 S_PAD 相同，即值是 1 的单元 #1 和单元 #M+1 这两个单元。

[0124] 如图中所述，关于单元号 S_PAD 具有值 1 的单元 #1 和单元 #M+1 这两个单元，能够通过参考序列号 SEQ 来在已经写入最后数据的单元（新单元）#1M+1 和在过去写入数据的单元（旧单元）#1 之间进行区分。

[0125] 在下次激活时，命令序列器部件 23 使用 CRC 作为是新单元的单元 #M+1 的管理页的误差检测码来进行误差检测，并且在未检测到误差的情况下（误差检测码正常的情况下），随着到作为新单元的单元 #M+1 的数据写入已经正常完成，作为旧单元的单元 #1 的管理页被擦除，并通过处于擦除状态（在图 4 中单元号 S_PAD 被设置为指示缓冲单元的值 0），单元 #1 被设置为缓冲单元。

[0126] 然后，在那之后，如图 3 中所述，进行到缓冲单元中的新数据写入。

[0127] 另一方面，在作为使用 CRC 作为是新单元的单元 #M+1 的管理页的误差检测码的误差检测而检测到误差的情况下（误差检测码中存在误差的情况下），随着到作为新单元的单元 #M+1 的数据写入还未正常完成，命令序列器部件 23 将存储器部件 24 的状态返回到例如进行到作为新单元的单元 #M+1 中的数据写入的先前状态。

[0128] 即，命令序列器部件 23 擦除作为新单元的单元 #M+1 的管理页，并通过处于擦除状

态（在图 4 中单元号 S_PAD 被设置为指示缓冲单元的值 0），单元 #M+1 被设置为缓冲单元。

[0129] 然后，在那之后，如图 3 中所述，进行新数据向缓冲单元中的写入。

[0130] 单侧验证

[0131] 图 5 是用于描述单侧验证的图。

[0132] 在此，如图 1 所述，读取器 / 写入器 10 具有产生在无线标签 20 的验证中使用的随机数的随机数产生部件 15，但是无线标签 20 不具有产生在读取器 / 写入器 20 的验证中使用的随机数的电路。

[0133] 因此，具有随机数产生部件 15 的读取器 / 写入器 10 进行单侧验证，其中使用由随机数产生部件 15 产生的随机数通过所谓的询问 (challenge) 和响应方法来验证无线标签 20。

[0134] 结果，读取器 / 写入器 10 的存储器部件 14 和无线标签 20 的存储器部件 24 存储单侧验证所需的信息。

[0135] 图 5 是图示存储在读取器 / 写入器 10 的存储器部件 14 和无线标签 20 的存储器部件 24 中的单侧验证所需的信息的图。

[0136] 作为对于由读取器 / 写入器 10 提供的服务唯一的密钥的唯一密钥 KG 存储在读取器 / 写入器 10 的存储器部件 14 中。

[0137] 另一方面，作为唯一 ID 的 ID 的单独 ID(＝ UID) 作为区分无线标签 20 的区分信息而被存储在无线标签 20 的存储器部件 24 中。

[0138] 此外，作为对于无线标签 20 唯一的密钥的单独密钥 UCK 被存储在无线标签 20 的存储器部件 24 中。

[0139] 使用单独 ID 和唯一密钥 KG 产生该单独密钥 UCK。即，通过对单独 ID 进行与唯一密钥 KG 对应的处理（例如使用唯一密钥 KG 的单独 ID 的加密）来产生单独密钥 UCK。

[0140] 从而，当与唯一密钥 KG 对应的处理由 $\{\}_{KG}$指示时，单独密钥 UCK 由等式 UCK ＝ $\{UID\}_{KG}$指示。

[0141] 在此，在无线标签 20 用在多个服务中的情况下，仅多个服务的单独密钥 UCK 的数量被存储在无线标签 20 的存储器部件 24 中。

[0142] 以下，为了简化描述，在无线标签 20 的存储器部件 24 中仅有一个用户块，从而，仅有一个能够使用无线标签 20 的服务。

[0143] 图 6 是描述在读取器 / 写入器 10 进行单侧验证的情况下读取器 / 写入器 10 和无线标签 20 的处理的图，在该单侧验证中，读取器 / 写入器 10 验证无线标签 20，并且无线标签 20 不进行读取器 / 写入器 10 的验证。

[0144] 例如，当在通过将无线标签 20 保持在读取器 / 写入器 10 之上而使得读取器 / 写入器 10 和无线标签 20 接近的状态下，读取器 / 写入器 10 和无线标签 20 之间的邻近通信开始。

[0145] 然后，在步骤 S11，读取器 / 写入器 10 的随机数产生部件 15 产生随机数 R 并将该随机数 R 提供给 RF 部件 12。

[0146] 在步骤 S12 中，RF 部件 12 将来自随机数产生部件 15 的随机数 R 经由天线 11 发送到无线标签 20，并且无线标签 20 的 RF 部件 22 经由天线 21 接收来自读取器 / 写入器 10 的 RF 部件 12 的随机数 R，并将该随机数 R 提供给命令序列器部件 23。

[0147] 在步骤 S21，命令序列器部件 23 使用来自 RF 部件 22 的随机数以及存储在存储器部件 24 中的单独密钥 UCK 来产生在读取器 / 写入器 10 和无线标签 20 之间的会话中使用的会话密钥 KS。

[0148] 即，命令序列器部件 23 通过对随机数 R 进行与单独密钥 UCK 对应的处理来产生会话密钥 $KS = \{R\}_{UCK}$。

[0149] 在那之后，在步骤 S22，命令序列器部件 23 通过控制 RF 部件 22 将通知已经接收到随机数 R 的响应从 RF 部件 22 发送到读取器 / 写入器 10。

[0150] 读取器 / 写入器 10 的 RF 部件 12 接收来自无线标签 20（的 RF 部件 22）的响应。然后，在步骤 S13，读取器 / 写入器 10 的 CPU 13 通过控制 RF 部件 12 将读命令发送到无线标签 20，该读命令请求无线标签 20 的单独 ID ＝ UID 以及例如用于检验单独 ID 的合法性的作为单独 ID 的加密数据的 MAC（消息验证码）值。

[0151] 在无线标签 20 中，RF 部件 22 接收来自读取器 / 写入器 10（的 RF 部件 12）的读命令，并将该读命令提供给命令序列器部件 23。

[0152] 在步骤 S23，命令序列器部件 23 根据来自 RF 部件 22 的读命令从存储器部件 24 读出单独 ID ＝ UID，并使用该单独 ID 和紧接在之前产生的会话密钥 KS 而产生 MAC 值 T ＝ MAC(KS，UID) 作为单独 ID 的加密数据（第三加密数据）。

[0153] 然后，命令序列器部件 23 将该单独 ID ＝ UID 和使用该单独 ID 产生的 MAC 值 T 提供给 RF 部件 22。

[0154] 在步骤 S24，RF 部件 22 将来自命令序列器部件 23 的单独 ID ＝ UID 和 MAC 值 T 发送到读取器 / 写入器 10。

[0155] 在此，作为使用单独 ID ＝ UID 和会话密钥 KS 产生 MAC 值 T ＝ MAC(KS，UID) 的方法，能够采用使用会话密钥 KS 以诸如 DES（数据加密标准）等的预定加密格式对单独 ID ＝ UID 加密的方法、使用单独 ID ＝ UID 和会话密钥 KS 计算预定哈希函数的方法等。

[0156] 在此，因为如果 MAC 值 T 能够检验（在此情况下是单独 ID ＝ UID）还未被篡改的消息就足够了，因此不需要能够解密原始信息（单独 ID ＝ UID 以及会话密钥 KS）。

[0157] 从而，在 MAC 值 T 的产生中能够使用例如单向 (one-way) 函数。

[0158] 读取器 / 写入器 10 的 RF 部件 12 从无线标签 20（的 RF 部件 22）接收单独 ID ＝ UID 和 MAC 值 T，并将该单独 ID ＝ UID 和 MAC 值 T 提供给 CPU 13。

[0159] 在步骤 S14 中，CPU 13 从存储器部件 14 读出唯一密钥 KG，并使用该唯一密钥 KG 以及来自 RF 部件 12 的单独 ID ＝ UID 来产生无线标签 20 的单独密钥 $UCK = \{UID\}_{KG}$。

[0160] 然后，在步骤 S15 中，CPU 13 使用单独密钥 UCK 和由随机数产生部件 15 紧接在之前产生的随机数 R 以与无线标签 20 相同的方式产生会话密钥 $KS = \{R\}_{UCK}$。

[0161] 在那之后，在步骤 S16，CPU 13 使用会话密钥 KS 和来自 RF 部件 12 的单独 ID ＝ UID 以与无线标签 20 相同的方式产生 MAC 值 T’ ＝ MAC(KS，UID) 作为单独 ID ＝ UID 的加密数据（第四加密数据）。

[0162] 然后，在步骤 S17，CPU 13 将如上产生的 MAC 值 T’ 与来自 RF 部件 12 的 MAC 值 T 相比较。

[0163] 作为 MAC 值 T’ 与 T 的比较结果，在 MAC 值 T’ 与 T 不相等的情况下，CPU 13 进行基于无线标签 20 的验证已经失败的预定的误差处理（例如在显示器（未示出）上显示验

证已经失败的处理），并且处理结束。

[0164] 从而，在验证已经失败的情况下，读取器 / 写入器 10 不进行对无线标签 20 的访问。

[0165] 另一方面，在 MAC 值 T’与 T 相等的情况下，CPU 13 基于无线标签 20 的验证已经成功，按照需要在以下进行数据向无线标签 20 的写入。

[0166] 如上所述，读取器 / 写入器 10 使用随机数，并且在进行单侧验证的情况下，能够防止合法的读取器 / 写入器 10 访问欺骗性的无线标签。

[0167] 但是，通过仅读取器 / 写入器 10 进行单侧验证，不能阻止欺骗性的读取器 / 写入器访问合法的无线标签 20。

[0168] 因此，无线标签 20 通过使用由读取器 / 写入器 10 进行的单侧验证的简化的验证方法进行读取器 / 写入器 20 的验证。

[0169] 无线标签 20 对读取器 / 写入器 10 的验证

[0170] 图 7 是描述在读取器 / 写入器 10 进行对于无线标签 20 的单侧验证并且无线标签 20 使用该单侧验证进行对读取器 / 写入器 10 的验证的情况下读取器 / 写入器 10 和无线标签 20 的处理的图。

[0171] 例如，当在通过将无线标签 20 保持在读取器 / 写入器 10 之上使得读取器 / 写入器 10 和无线标签 20 接近的状态下时，读取器 / 写入器 10 和无线标签 20 之间的邻近通信开始。

[0172] 然后，在步骤 S51，读取器 / 写入器 10 的随机数产生部件 15 产生随机数 R 并将该随机数 R 提供给 RF 部件 12。

[0173] 在步骤 S52，RF 部件 12 将来自随机数产生部件 15 的随机数 R 发送到无线标签 20，并且无线标签 20 的 RF 部件 22 接收来自读取器 / 写入器 10 的 RF 部件 12 的随机数 R，并将该随机数 R 提供给命令序列器部件 23。

[0174] 在步骤 S71，命令序列器部件 23 使用来自 RF 部件 22 的随机数 R 和存储在存储器部件 24 中的单独密钥 UCK 来产生会话密钥 KS。

[0175] 在那之后，在步骤 S72，命令序列器部件 23 通过控制 RF 部件 22 将通知已经接收到随机数 R 的响应从 RF 部件 23 发送到读取器 / 写入器 10。

[0176] 读取器 / 写入器 10 的 RF 部件 12 接收来自无线标签 20（的 RF 部件 22）的响应。然后，在步骤 S53，读取器 / 写入器 10 的 CPU 13 通过控制 RF 部件 12 将读命令发送到无线标签 20，该读命令请求无线标签 20 的单独 ID ＝ UID、用于检验单独 ID 的合法性的 MAC 值以及序列号 SEQ（的读出）。

[0177] 在此，存储器部件 24 的逻辑格式如图 2 所示，并且存在存储每个单元的管理信息的管理页，从而，在存在被包括在每个单元的管理信息中的序列号 SEQ 的情况下，在步骤 S53，CPU 13 使用读命令而请求的序列号 SEQ 是进行数据写入的目标单元的序列号 SEQ。

[0178] 在无线标签 20 中，RF 部件 22 接收来自读取器 / 写入器 10（的 RF 部件 12）的读命令，并将该读命令提供给命令序列器部件 23。

[0179] 在步骤 S73，命令序列器部件 23 根据来自 RF 部件 22 的读命令从存储器部件 24 读出单独 ID ＝ UID 和目标单元的序列号 SEQ。

[0180] 此外，在步骤 S73，命令序列器部件 23 使用从存储器部件 24 读出的单独 ID 以及紧

接在之前产生的会话密钥 KS 来产生 MAC 值 T = MAC(KS,UID) 作为单独 ID = UID 的加密数据（第三加密数据）。

[0181] 然后，命令序列器部件 23 将单独 ID = UID、序列号 SEQ = X 以及 MAC 值 T 提供给 RF 部件 22。

[0182] 在步骤 S74，RF 部件 22 将来自命令序列器部件 23 的单独 ID = UID 和序列号 SEQ = X 以及 MAC 值 T 发送到读取器 / 写入器 10。

[0183] 读取器 / 写入器 10 的 RF 部件 12 接收来自无线标签 20（的 RF 部件 22）的单独 ID = UID、序列号 SEQ = X 以及 MAC 值 T，并将该单独 ID = UID、序列号 SEQ = X 以及 MAC 值 T 提供给 CPU 13。

[0184] 在步骤 S54，CPU 13 从存储器部件 14 中读出唯一密钥 KG 并使用该唯一密钥 KG 以及来自 RF 部件 12 的单独 ID = UID 来产生无线标签 20 的单独密钥 $UCK = \{UID\}_{KG}$。

[0185] 然后，在步骤 S55，CPU 13 使用该单独密钥 UCK 以及紧接在之前由随机数产生部件 15 产生的随机数 R 以与无线标签 20 相同的方式产生会话密钥 $KS = \{R\}_{UCK}$。

[0186] 在那之后，在步骤 S56 中，CPU 13 使用该会话密钥 KS 和来自 RF 部件 12 的单独 ID = UID 来产生 MAC 值 T' = MAC(KS,UID) 作为单独 ID = UID 的加密数据（第四加密数据）。

[0187] 然后，在步骤 S57，CPU 13 将如上产生的 MAC 值 T' 与来自 RF 部件 12 的 MAC 值 T 相比较。

[0188] 作为 MAC 值 T' 与 T 的比较结果，在 MAC 值 T' 与 T 不相等的情况下，CPU 13 进行基于无线标签 20 的验证已经失败的预定的误差处理，并且处理结束。

[0189] 从而，在验证已经失败的情况下，读取器 / 写入器 10 不进行对无线标签 20 的访问。

[0190] 另一方面，在 MAC 值 T' 与 T 相等的情况下，CPU 13 基于无线标签 20 的验证已经成功，产生例如作为在无线标签 20 对读取器 / 写入器 10 的验证中使用的加密数据的 MAC 值 W。

[0191] 即，CPU 13 使用基于来自无线标签 20 的序列号 SEQ = X 的值和作为被写入到目标单元中的目标数据的写目标数据 D，产生例如作为基于序列号 SEQ = X 的值和写目标数据 D 的加密数据（第一加密数据）的 MAC 值 W。

[0192] 具体地，CPU 13 产生例如会话密钥 KS、目标单元的单元号 S_PAD = m、来自无线标签 20 的序列号 SEQ = X 以及写目标数据 D 的 MAC 值 W = MAC(KS,S_PAD = m,SEQ = X,D)，作为基于序列号 SEQ = X 的值和写目标数据 D 的加密数据。

[0193] 然后，CPU 13 将请求写入写目标数据 D 的写命令、写目标数据 D、目标单元的单元号 S_PAD = m 以及 MAC 值 W = MAC(KS,S_PAD = m,SEQ = X,D) 提供给 RF 部件 12。

[0194] 在步骤 S59，读取器 / 写入器 10 的 RF 部件 12 将来自 CPU 13 的写命令、写目标数据 D、目标单元的单元号 S_PAD = m 以及 MAC 值 W 发送到无线标签 20。

[0195] 在无线标签 20 中，来自读取器 / 写入器 10（的 RF 部件 12）的写命令、写目标数据 D、目标单元的单元号 S_PAD = m 以及 MAC 值 W 由 RF 部件 22 接收并被提供给命令序列器部件 23。

[0196] 在步骤 S75，命令序列器部件 23 使用基于紧接在之前发送到读取器 / 写入器 10 的序列号 SEQ = X 的值和由 RF 部件 22 接收的写目标数据 D 来产生 MAC 值 W' 作为基于序列

号 SEQ = X 的值和由 RF 部件 22 接收写目标数据 D 的加密数据（第二加密数据）。

[0197] 即，命令序列器部件 23 产生紧接在之前产生的会话密钥 KS、目标单元的单元号 S_PAD = m、紧接在之前发送到读取器 / 写入器 10 的序列号 SEQ = X 以及由 RF 部件 22 接收的写目标数据 D 的 MAC 值 W' = MAC(KS, S_PAD = m, SEQ = X, D)，作为基于序列号 SEQ = X 的值和写目标数据 D 的加密数据。

[0198] 然后，在步骤 S76，命令序列器部件 23 将如上产生的 MAC 值 W' 与来自 RF 部件 22 的 MAC 值 W 相比较。

[0199] 作为 MAC 值 W' 与 W 的比较结果，在 MAC 值 W' 与 W 不相等的情况下，命令序列器部件 23 基于读取器 / 写入器 10 的验证已经失败而结束处理。

[0200] 从而，在此情况下，无线标签 20 不进行来自读取器 / 写入器 10 的写目标数据 D 的写入，并且不响应于在那之后的来自读取器 / 写入器 10 的访问。

[0201] 另一方面，在 MAC 值 W' 与 W 相等的情况下，基于读取器 / 写入器 10 的验证已经成功，无线标签 20 的命令序列器部件 23 在步骤 S77 将由 RF 部件 22 接收的写目标数据 D（即从读取器 / 写入器 10 发送的写目标数据 D）写入到（作为）目标单元（的缓冲单元）中。

[0202] 在那之后，在步骤 S78，命令序列器部件 23 执行更新（作为）目标单元（的缓冲单元）的管理页的管理信息（即，作为目标单元的管理信息的单元号 S_PAD）和序列号 SEQ = X，并计算误差检测码的处理。

[0203] 然后，在步骤 S79，命令序列器部件 23 通过控制 RF 部件 22 将通知写入已经完成的响应从 RF 部件 22 发送到读取器 / 写入器 10。

[0204] 读取器 / 写入器 10 的 RF 部件 12 接收来自无线标签 20（的 RF 部件 22）的响应。

[0205] 如上所述，无线标签 20 的 RF 部件 22 将序列号 SEQ = X 发送到读取器 / 写入器 10，并且读取器 / 写入器 10 的 CPU 13 使用基于从无线标签 20 发送的序列号 SEQ 的值和被写入到无线标签 20 的存储器部件 24 中的写目标数据 D 而产生 MAC 值 W = MAC(KS, S_PAD = m, SEQ = X, D)（第一加密数据）。

[0206] 此外，读取器 / 写入器 10 的 RF 部件 12 将该 MAC 值 W 和写目标数据 D 发送到无线标签 20，并且无线标签 20 的 RF 部件 22 接收该 MAC 值 W 和写目标数据 D。

[0207] 另外，无线标签 20 的命令序列器部件 23 使用基于（发送到读取器 / 写入器 10 的）序列号 SEQ 的值和由 RF 部件 22 接收的写目标数据 D 产生 MAC 值 W' = MAC(KS, S_PAD = m, SEQ = X, D)（第二加密数据）。

[0208] 然后，无线标签 20 的命令序列器部件 23 仅当 MAC 值 W' 和 W 相匹配时，将由 RF 部件 22 接收的写目标数据 D 写入到存储器部件 24（的目标单元）中，并且更新存储在存储器部件 24 中的（目标单元中的）序列号 SEQ。

[0209] 从而，无线标签 20 能够通过比较 MAC 值 W' 和 W 来进行读取器 / 写入器 10 是否是合法设备的验证，此外，在验证成功的情况下，能够将写目标数据 D 写入到存储器部件 24 中。

[0210] 结果，关于无线标签 20，能够确保安全性，即防止欺骗性读取器 / 写入器欺骗性地重写在存储器部件 24 中的数据。

[0211] 另外，与进行相互验证的情况相比，能够缩短读取器 / 写入器 10 将数据写入到无线标签 20 中所需的时间（从读取器 / 写入器 10 和无线标签 20 开始邻近通信时到写目标

数据 D 被写入到存储器部件 24 中的时间）。

[0212] 即，在进行读取器 / 写入器 10 和无线标签 20 之间的相互验证的情况下，进行需要两个交易业务 (transaction) 的相互验证 :读取器 / 写入器 10 进行对无线标签 20 的验证的交易业务和无线标签 20 进行对读取器 / 写入器 10 的验证的交易业务，并且在相互验证成功之后，写目标数据 D 被从读取器 / 写入器 10 发送到无线标签 20 并被写入到无线标签 20 的存储器部件 24 中。

[0213] 另一方面，如图 7 所示，在读取器 / 写入器 10 使用单侧验证进行对无线标签 20 的验证并且无线标签 20 通过使用单侧验证的简化验证方法进行对读取器 / 写入器 10 的验证的情况下（以此方式在读取器 / 写入器 10 和无线标签 20 之间的验证以下被称为简化验证），在读取器 / 写入器 10 进行单侧验证之后，写目标数据 D 和 MAC 值 W 被从读取器 / 写入器 10 发送到无线标签 20。

[0214] 然后，在无线标签 20 中，使用 MAC 值 W 进行在 MAC 值 W 的产生中使用的序列号 SEQ 和写目标数据 D 的验证 (MAC 值 W 和 W’的比较），并且如果序列号 SEQ 和写目标数据 D 没有问题（如果 MAC 值 W 和 W’相匹配），则基于写目标数据 D 没有被篡改以及读取器 / 写入器 10 的验证成功，将写目标数据 D 写入到存储器部件 24 中。

[0215] 从而，因为写目标数据 D 被从读取器 / 写入器 10 发送到无线标签 20 作为在无线标签 20 对读取器 / 写入器 10 的验证（以及对写目标数据 D 的检验）中使用的数据，因此在无线标签 20 对读取器 / 写入器 10 的验证成功之后不需要将写目标数据 D 从读取器 / 写入器 10 发送到无线标签 20。

[0216] 这样，在该简化验证中，与在相互验证成功之后将写目标数据 D 从读取器 / 写入器 10 发送到无线标签 20 的情况相比，能够缩短读取器 / 写入器 10 将数据写入到无线标签 20 中所需的时间。

[0217] 另外，因为在每次数据被写入到无线标签 20 的存储器部件 24 中时在 MAC 值 W 和 W’的产生中使用的序列号 SEQ 规律地更新值，因此即使存在对从读取器 / 写入器 10 发送到无线标签 20 的 MAC 值 W 的窃听并且使用该 MAC 值 W 进行关于无线标签 20 的重放攻击 (replay attack)，在该重放攻击中使用的 MAC 值 W 也不与使用在无线标签 20 中的更新之后的序列号 SEQ 产生的 MAC 值 W’相匹配。

[0218] 从而，能够防止重放攻击。

[0219] 另外，在图 7 中（并以与稍后描述的图 8 中相同的方式），在 MAC 值 W 和 W’的产生中使用会话密钥 KS、目标单元的单元号 S_PAD ＝ m、序列号 SEQ ＝ X 以及写目标数据 D，但是能够使用会话密钥 KS、序列号 SEQ ＝ X 以及写目标数据 D 而不使用目标单元的单元号 S_PAD ＝ m 来产生 MAC 值 W 和 W’。

[0220] 但是，也使用目标单元的单元号 S_PAD ＝ m，通过产生 MAC 值 W 和 W’，能够防止从外部篡改单元号 S_PAD ＝ m，即写目标数据 D 被写入的写目的地单元的欺骗性改变。

[0221] 图 8 是描述读取器 / 写入器 10 的另一处理和无线标签 20 进行的简化验证的图。

[0222] 在图 7 的简化验证的处理中，序列号 SEQ ＝ X 本身用作在 MAC 值 W 和 W’的产生中使用的基于序列号 SEQ 的值，但是，作为在 MAC 值 W 和 W’的产生中使用的基于序列号 SEQ 的值，另外，能够采用在更新后的序列号 SEQ ＝ X+1。

[0223] 但是，在使用更新后的序列号 SEQ ＝ X+1 产生 MAC 值 W 和 W’的情况下，需要在读

取器 / 写入器 10 中实行其中每次数据被写入到存储器部件 24 中时规律地更新值的序列号 SEQ 的更新规则（使得读取器 / 写入器 10 识别序列号 SEQ 的更新规则）。

[0224] 在图 8 中，在步骤 S101 到 S109，读取器 / 写入器 10 以与图 7 中的步骤 S51 到 S59 的每个相同的方式进行处理，并在步骤 S121 到 S129 中，无线标签 20 以与图 7 中的步骤 S71 到 S79 的每个相同的方式进行处理。

[0225] 但是，在与图 7 中的步骤 S58 对应的步骤 S108 中，读取器 / 写入器 10 确定其中来自无线标签 20 的序列号 SEQ = X 被更新的更新后的序列号 SEQ = X+1，并且使用更新后的序列号 SEQ = X+1 代替序列号 SEQ = X 本身来产生 MAC 值 W = MAC(KS, S_PAD = m, SEQ = X+1, D)。

[0226] 另外，在与图 7 中的步骤 S75 对应的步骤 S125 中，无线标签 20 确定其中目标单元的序列号 SEQ = X 被更新的更新后的序列号 SEQ = X+1，并且使用该更新后的序列号 SEQ = X+1 代替序列号 SEQ = X 本身来产生 MAC 值 W' = MAC(KS, S_PAD = m, SEQ = X+1, D)。

[0227] 如上所述，在使用更新后的序列号 SEQ = X+1 产生 MAC 值 W 和 W' 的情况下，即使存在对序列号 SEQ = X 的窃听，因为如果不知道序列号 SEQ 的更新规则，则不能产生与在无线标签 20 中产生的 MAC 值 W' 相匹配的 MAC 值 W，所以比在使用序列号 SEQ 本身产生 MAC 值 W 和 W' 的情况下更能改善安全性。

[0228] 存储器部件 24 的逻辑格式的另一实施例

[0229] 图 9 是描述图 1 的无线标签 20 的存储器部件 24 的逻辑格式的另一实施例的图。

[0230] 图 9 的逻辑格式具有 :与图 2 的情况相同，存储器部件 24 的存储器区的一部件是分配给服务的一个或多个用户块。

[0231] 但是，图 9 的逻辑格式与图 2 的情况不同在于 :存储器部件 24 的存储器区的另一部件是存储管理信息的管理块，在图 2 中的情况下管理信息被存储在页（管理页）中。

[0232] 在此，在图 2 中，单元由多页配置，因为在单元中需要具有存储数据的一页或多页（数据页）和一个管理页，而在图 9 中，因为管理信息被存储在管理块中并且不需要管理页，因此能够以一页或多页配置单元。

[0233] 在图 9 中，单元由一页配置。

[0234] 从而，在图 9 中，单元等效于页。

[0235] 另外，在图 9 中，数据和作为数据的误差检测码的 CRC 被存储在用户块的单元（其等效于页）中。

[0236] 管理块由例如数量是作为用户块的数量的两倍的数量的 M' 个单元（或图 9 中的页）配置。

[0237] 从而，存储器部件 24 被设置为具有一个用户块并且管理块具有两个单元。

[0238] 每个用户块的管理信息被存储在管理块中。一个用户块的管理信息被存储在管理块的两个单元中。

[0239] 在此，存储了一个用户块的管理信息的管理块的两个单元是与用户块对应的管理块的两个单元。

[0240] 在此，关注某一用户块，在与所关注的某一用户块对应的管理块的两个单元（页）的每个中，存储了作为该某用户块的管理信息的配置该某用户块的 M+1 个单元的单元号 S_PAD、一个序列号以及作为 (M+1 个单元的单元号 S_PAD 和该一个序列号的）误差检测码的

CRC。

[0241] 在此，在对应于该某用户块的管理块的两个单元中，每次数据被写入该某用户块中时，在数据写入之后，交替地写入该某用户块的管理信息。

[0242] 从而，在与该某用户块对应的管理块的两个单元中的单元之一中，存储该某用户块的最新管理信息，并且在另一单元中，存储紧接在该最新管理信息写入之前的管理信息。

[0243] 如上所述，针对存储器讹误的手段是可能的，因为通过每次数据被写入该某用户块中时该某用户块的管理信息被交替写入与该某用户块对应的管理块的两个单元中，而存储某用户块的最新管理信息和紧接在该最新管理信息之前写入之前的管理信息。

[0244] 在此，在与该某用户块对应的管理块的两个单元（页）的每个中存储 M+1 个单元的单元号 S_PAD 的存储器区被划分成 M+1 个存储器区（以下称为单元号区），其存储用于指定配置该某用户块的 M+1 个单元的单元号 S_PAD 的信息（以下称为单元号指定信息）。

[0245] 然后，采用值 m 作为配置某用户块的 M+1 个单元 #1 到 #M+1 中的第 m 单元的单元号指定信息，并在 M+1 个单元号区中从前面起的第 i 单元号区中存储单元号 S_PAD 是值 i 的单元 #m 的单元号指定信息 #m。

[0246] 从而，在单元号指定信息 #m 被存储在 M+1 个单元号区中从前面起的第 i 单元号区中的情况下，在配置某用户块的 M+1 个单元 #1 到 #M+1 中，第 m 个单元 #m 的单元号 S_PAD 是值 i。

[0247] 如上所述，在图 9 中，因为单元 #m 的单元号 S_PAD 由被写入到第 i 单元号区中的单元 #m 的单元号指定信息 #m 指定为值 i，在实践中（等效地），能够将单元 #m 的单元号 S_PAD#i 包括在管理信息中。

[0248] 在此，在图 9 中，如上所述，因为一个序列号 SEQ 被包括在某用户块的管理信息中，因此即使数据被写入该某用户块的任一单元中时也更新序列号 SEQ。

[0249] 即，在图 2 中，因为存在每个单元的管理信息并且一个序列号 SEQ 被包括在管理信息中，因此每次数据被写入到给定单元中时更新被包括在给定单元的管理信息中的序列号 SEQ。

[0250] 另一方面，在图 9 中，因为存在每个用户块的管理信息并且一个序列号 SEQ 被包括在管理信息中，因此即使数据被写入到用户块的任一单元中，被包括在给定单元块的管理信息中的序列号 SEQ 被更新（在每次数据被写入到用户块中时更新）。

[0251] 在此，能够关于存储器部件 24 仅提供一个序列号 SEQ。在此情况下，即使数据被写到存储器部件 24 的任意用户块的任意单元中，关于存储器部件 24 仅提供了一个的序列号 SEQ 也被更新。

[0252] 在存储器部件 24 具有图 9 的逻辑格式的情况下，以与图 2 的情况相同的方式，命令序列器部件 23 进行对数据向存储器部件 24 的写入的控制。

[0253] 即，例如，紧接在进行数据写入之前（写入之前），在某用户块的 M+1 个单元 #1 到 #M+1 中，例如，第 M+1 个单元 #M+1 是缓冲单元并且第 1 到第 M 单元￥1 到 #M 是数据单元。

[0254] 另外，数据单元 #m 的单元号 S_PAD 被设置为值 m，并且该某用户块的（被包括在管理信息中的）序列号 SEQ 被设置为值 X。

[0255] 然后，在此，例如，请求到（该某用户块的）单元号 S_PAD 是值 1 的单元的数据写入的写命令被与数据一起从读取器 / 写入器 10 发送到无线标签 20。

[0256] 在此情况下，命令序列器部件 23 根据来自读取器 / 写入器 10 的写命令，将与写命令一起发送的数据写入到作为缓冲单元的单元 #M+1 中，并且不写入到作为要进行写入的目标的单元的目标单元中，即，不写入到单元号 S_PAD 具有值 1 的单元 #1（由写命令请求写入的具有单元号 S_PAD 的单元）。

[0257] 在那之后，命令序列器部件 23 更新该某用户块的管理信息。

[0258] 即，作为某用户块的管理信息，最新管理信息（以下称为最新管理信息）和紧接在该最新管理信息被写入之前的管理信息（以下称为先前管理信息）被存储在存储器部件 24 中，如上所述。

[0259] 在此，管理信息 C#t 被设置为作为某用户块的最新管理信息存储在存储器部件 24 中，并且管理信息 C#t-1 被设置为作为某用户块的先前管理信息存储在存储器部件 24 中。

[0260] 命令序列器部件 23 更新管理信息 C#t 使得作为缓冲单元的单元 #M+1 的单元号 S_PAD 被设置为与作为目标单元的单元 #1 的单元号 S_PAD ＝ 1 相同的单元号 S_PAD ＝ 1，并且被设置为新缓冲单元的单元 #1 的单元号 S_PAD 被设置为指示缓冲单元的值 0。

[0261] 此外，命令序列器部件 23 更新包括管理信息 C#t 的序列号 SEQ 并计算新的误差检测码。

[0262] 然后，当作为以上的结果而获得的管理信息被设置为指示管理信息 C#t+1 时，命令序列器部件 23 以将管理信息 C#t+1 重写作为存储器部件 24 的先前管理信息的管理信息 C#t-1 作为该某用户块的管理信息的格式进行写入。

[0263] 结果，管理信息 C#t+1 变为该某用户块的最新管理信息，并且管理信息 C#t 变为该某用户块的先前管理信息。

[0264] 在此，本发明的实施例不限于上述实施例，并且在不脱离本发明的概念的范围内，各种修改是可能的。

[0265] 即，例如，在各实施例中，采用 EEPROM 作为是非易失性存储器的存储器部件 24，但是能够采用不同于 EEPROM 的诸如 FeRAM（铁电随机存取存储器）的非易失性存储器作为存储器部件 24。

[0266] 另外，在各实施例中，不同于数据单元的缓冲单元被提供在存储器部件 24 中，但是可以不提供缓冲单元。但是，在不提供缓冲单元的情况下，难以具有针对存储器讹误的手段。

[0267] 在此，在根据对称密码算法的相互验证中，读取器 / 写入器发送专用验证命令，该专用验证命令是用于进行诸如使无线标签产生随机数并将其中该随机数被加密的加密数据发送到读取器 / 写入器的处理的专用命令。

[0268] 从而，需要无线标签翻译这样的专用命令。

[0269] 另外，在进行根据对称密码算法的相互验证的情况下，使用通过使用随机数产生的加密密钥来加密数据并在相互验证之后在读取器 / 写入器和无线标签之间交换该数据以便防止窃听。

[0270] 因为在数据被加密和交换的情况下还存在数据的解密，因此在不解密而交换数据（以纯文本）的情况下需要具有单独的命令。

[0271] 即，在数据被加密并交换的情况下，需要用于进行数据解密的数据交换的专用加密读命令和写命令以及用于进行数据未解密的数据交换的正常读命令和写命令。

[0272] 关于此，因为以纯文本而不进行根据对称密码算法的相互验证来在读取器 / 写入器 10 和无线标签 20 之间交换数据，因此不需要专用的验证命令和专用的加密读命令和写命令。

[0273] 从而，能够降低要由无线标签 20 翻译的命令的数量，结果，作为无线标签 20 的命令序列器部件 23，能够采用 PLC（可编程逻辑控制器）而不采用诸如 CPU 之类的高级处理器。

[0274] 本申请包含与于 2010 年 6 月 10 日在日本专利局提交的日本优先权专利申请 JP 2010-133180 中的公开的主题有关的主题，通过引用将其全部内容合并于此。

[0275] 本领域技术人员应当理解，取决于设计要求和其他因素，可以发生各种修改、组合、部分组合和变更，只要其在所附权利要求或其等效物的范围内即可。

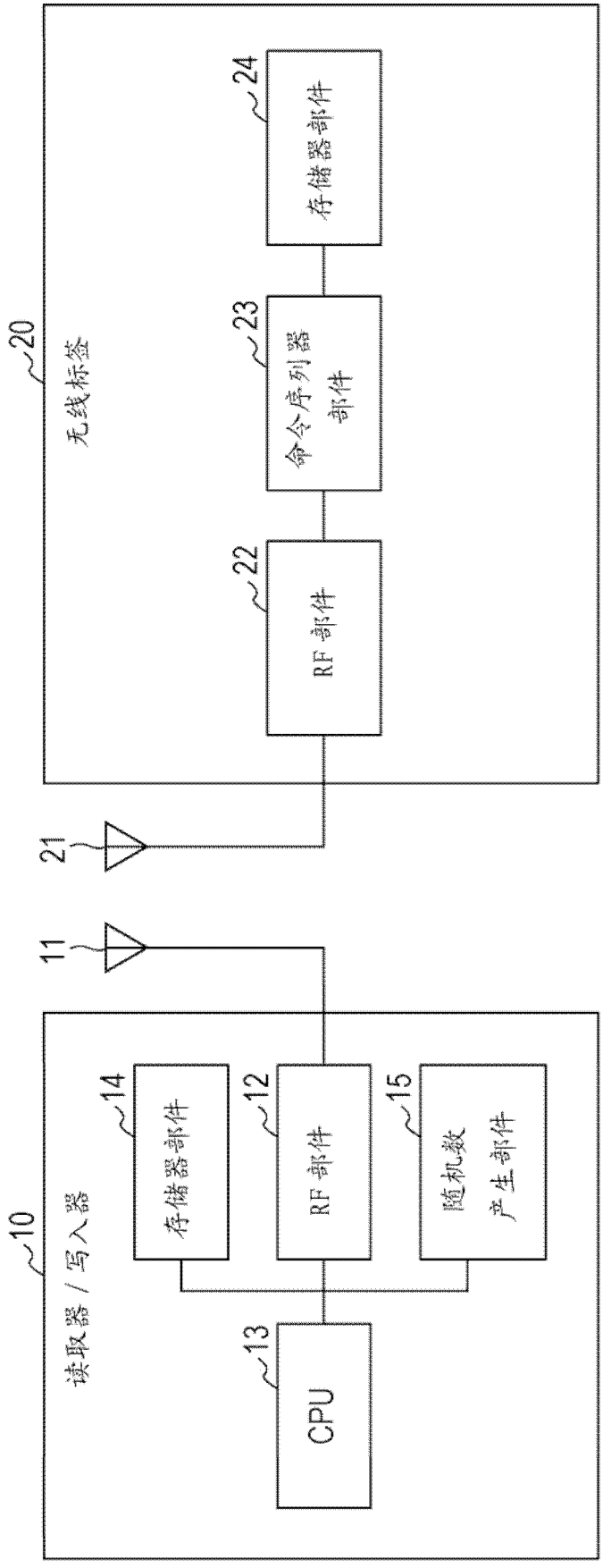

20
无线标签
24
存储器部件
23
命令序列器部件
22
RF 部件
21
11
10
读取器 / 写入器
14
存储器部件
12
RF 部件
15
随机数产生部件
13
CPU

图 1

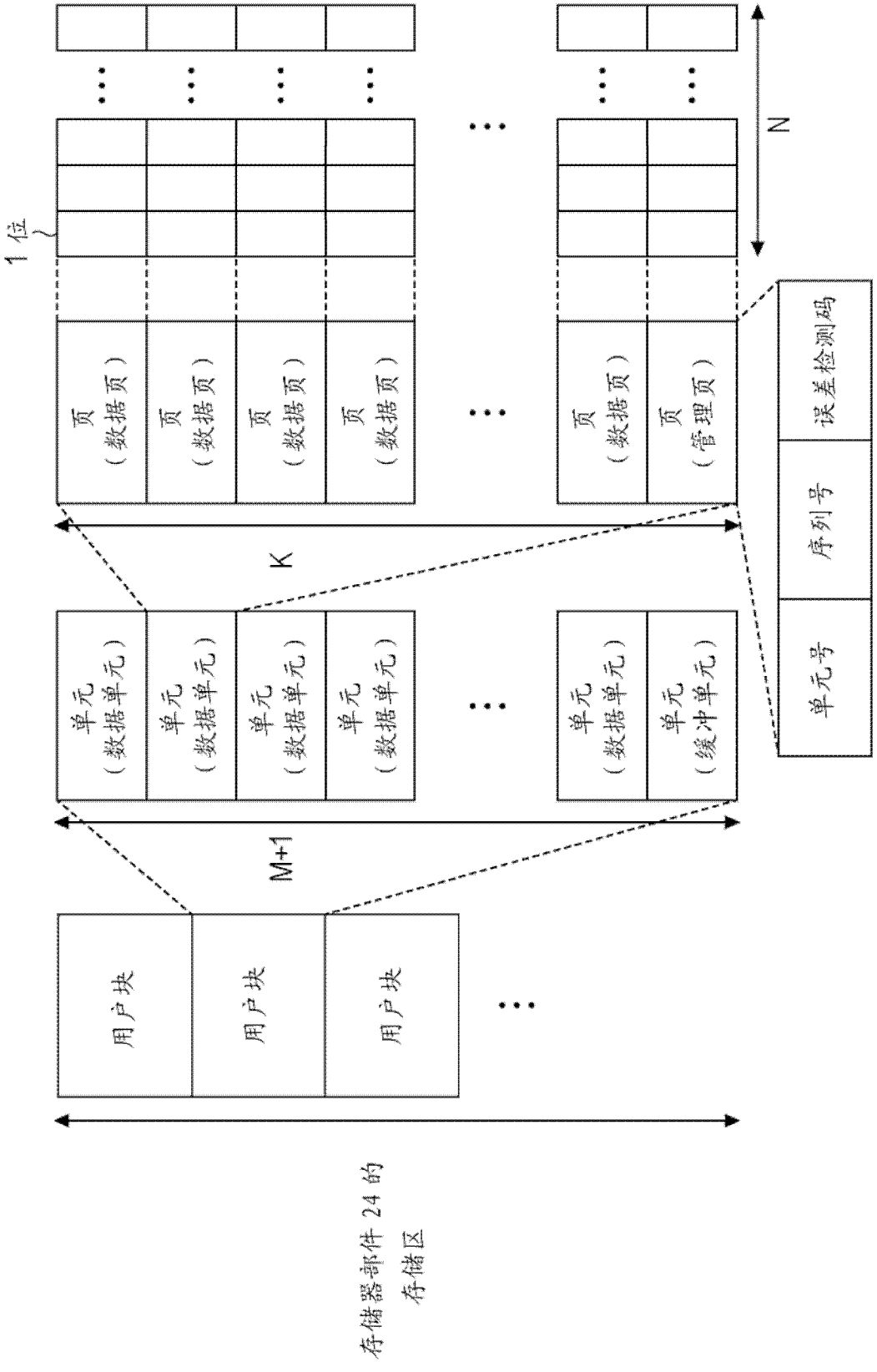

1 位
N
页（数据页）
页（数据页）
页（数据页）
页（数据页）
页（数据页）
页（管理页）
K
单元（数据单元）
单元（数据单元）
单元（数据单元）
单元（数据单元）
单元（数据单元）
单元（缓冲单元）
M+1
单元号
序列号
误差检测码
用户块
用户块
用户块
存储器部件 24 的存储区

图 2

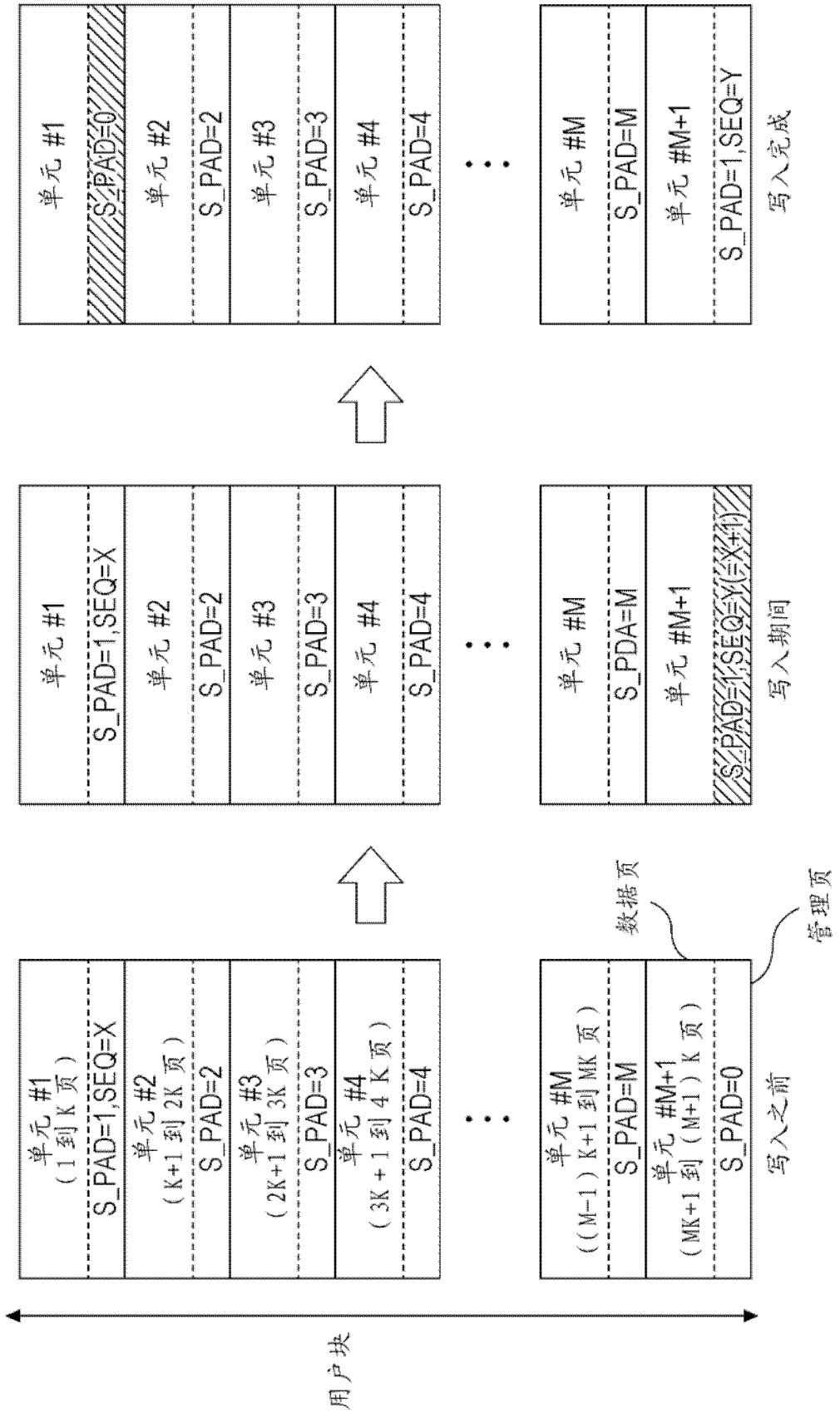

单元 #1
S_PAD=0
单元 #2
S_PAD=2
单元 #3
S_PAD=3
单元 #4
S_PAD=4
单元 #M
S_PAD=M
单元 #M+1
S_PAD=1,SEQ=Y
写入完成
单元 #1
S_PAD=1,SEQ=X
单元 #2
S_PAD=2
单元 #3
S_PAD=3
单元 #4
S_PAD=4
单元 #M
S_PDA=M
单元 #M+1
写入期间
单元 #1
（1 到 K 页）
单元 #2
（K+1 到 2K 页）
单元 #3
（2K+1 到 3K 页）
单元 #4
（3K + 1 到 4 K 页）
单元 #M
（（M−1）K+1 到 MK 页）
单元 #M+1
（MK+1 到（M+1）K 页）
S_PAD=0
数据页
管理页
写入之前
用户块

图 3

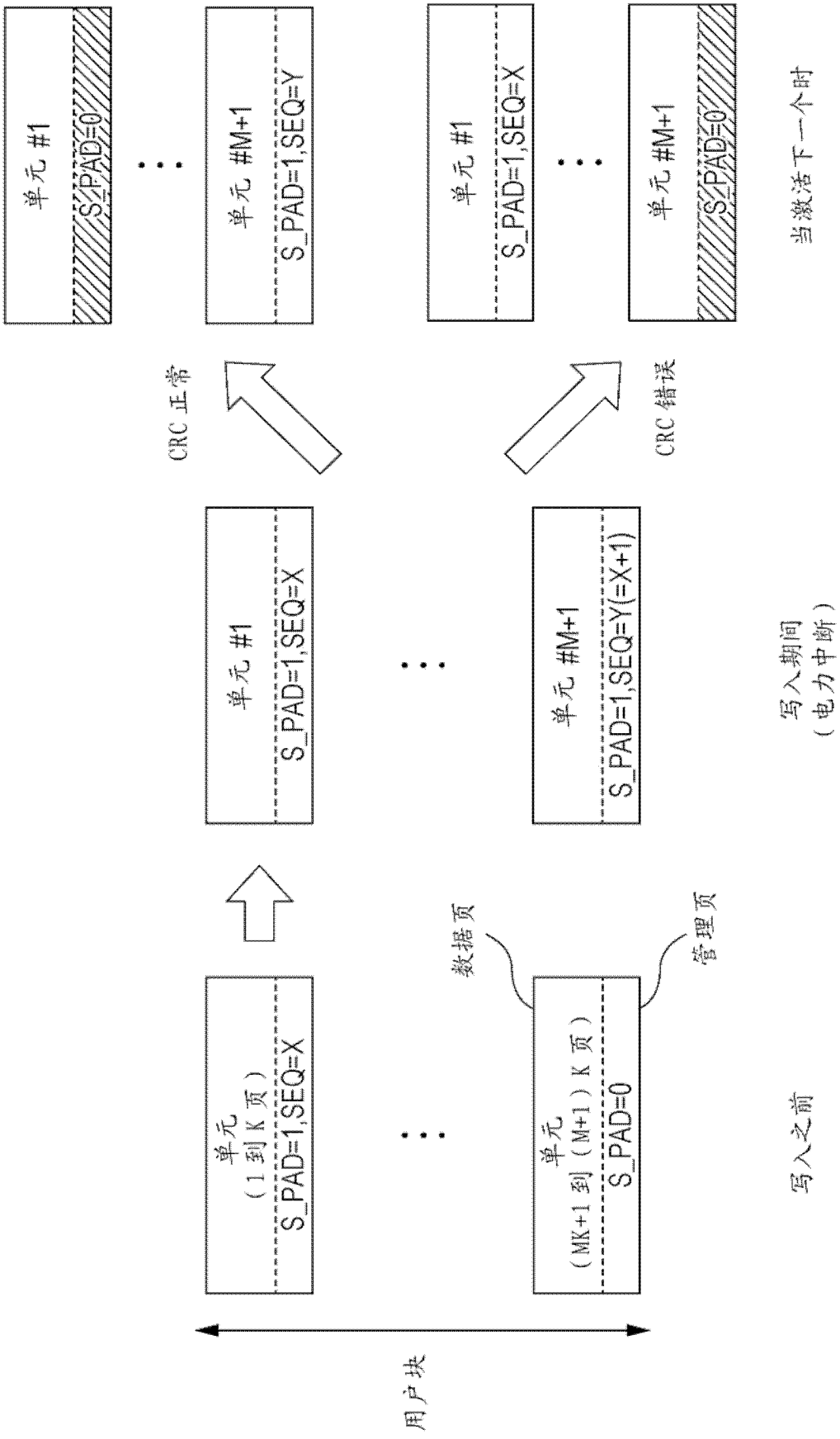

用户块
单元
（1到K页）
S_PAD=1,SEQ=X
单元
（MK+1到（M+1）K页）
S_PAD=0
数据页
管理页
写入之前
单元 #1
S_PAD=1,SEQ=X
单元 #M+1
S_PAD=1,SEQ=Y(=X+1)
写入期间
（电力中断）
CRC 正常
CRC 错误
单元 #1
S_PAD=1,SEQ=X
单元 #M+1
S_PAD=0
单元 #1
S_PAD=1,SEQ=Y
单元 #M+1
S_PAD=0
当激活下一个时

图 4

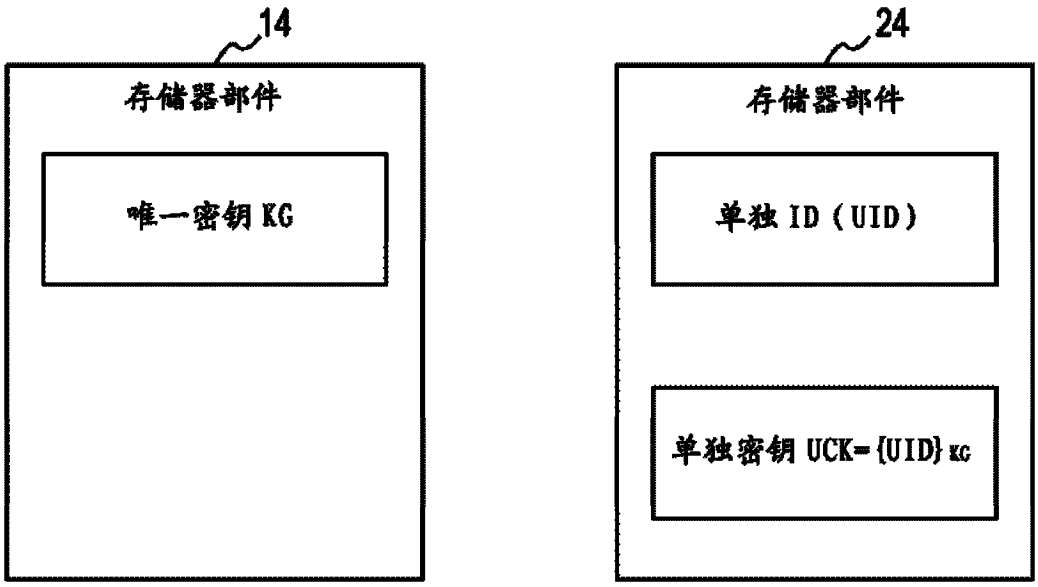


图 5

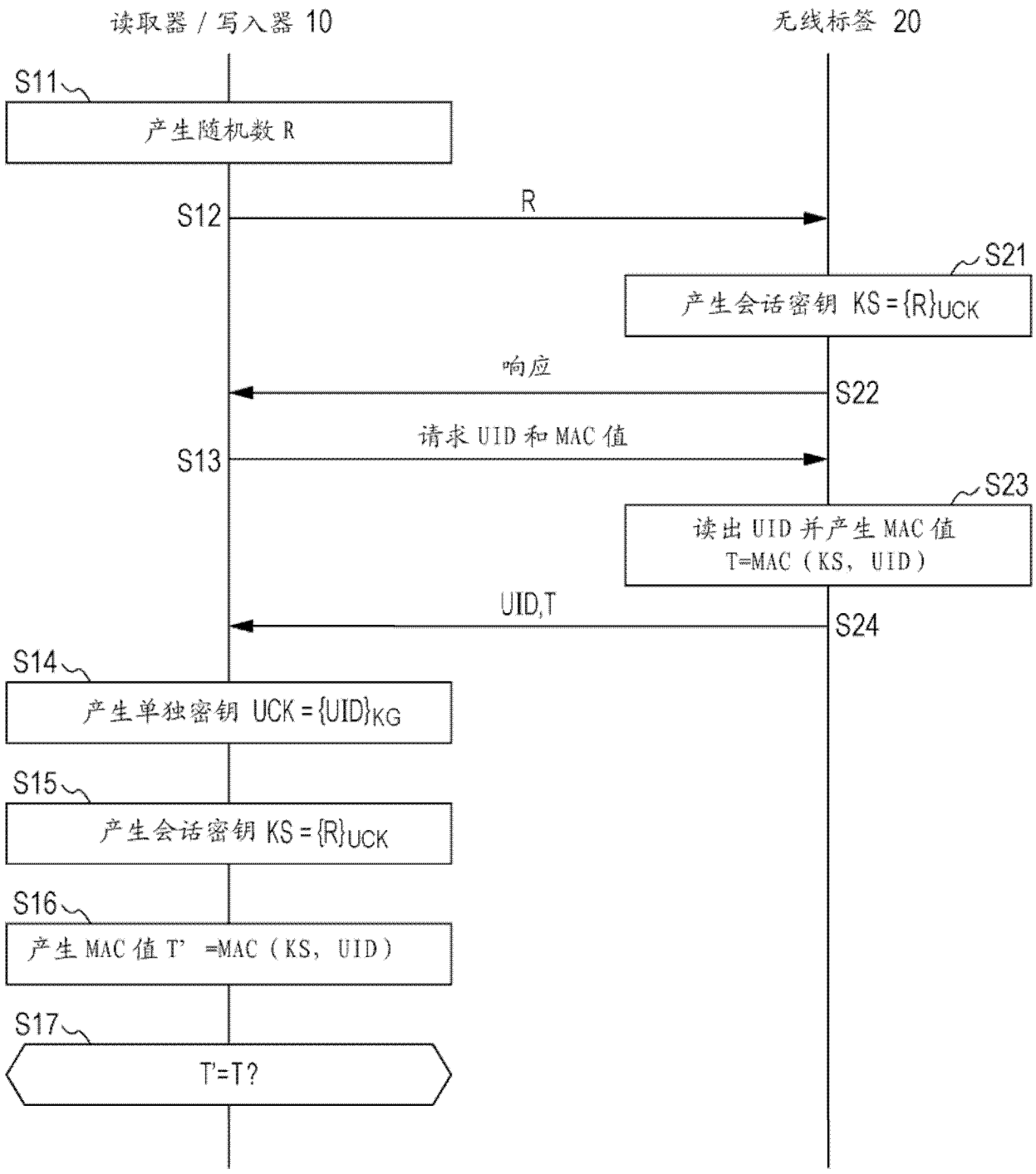

读取器 / 写入器 10
无线标签 20
S11
产生随机数 R
S12
R
S21
产生会话密钥 KS = {R}UCK
响应
S22
请求 UID 和 MAC 值
S13
S23
读出 UID 并产生 MAC 值
T=MAC（KS，UID）
UID,T
S24
S14
产生单独密钥 UCK = {UID}KG
S15
产生会话密钥 KS = {R}UCK
S16
产生 MAC 值 T' =MAC（KS，UID）
S17
T'=T?

图 6

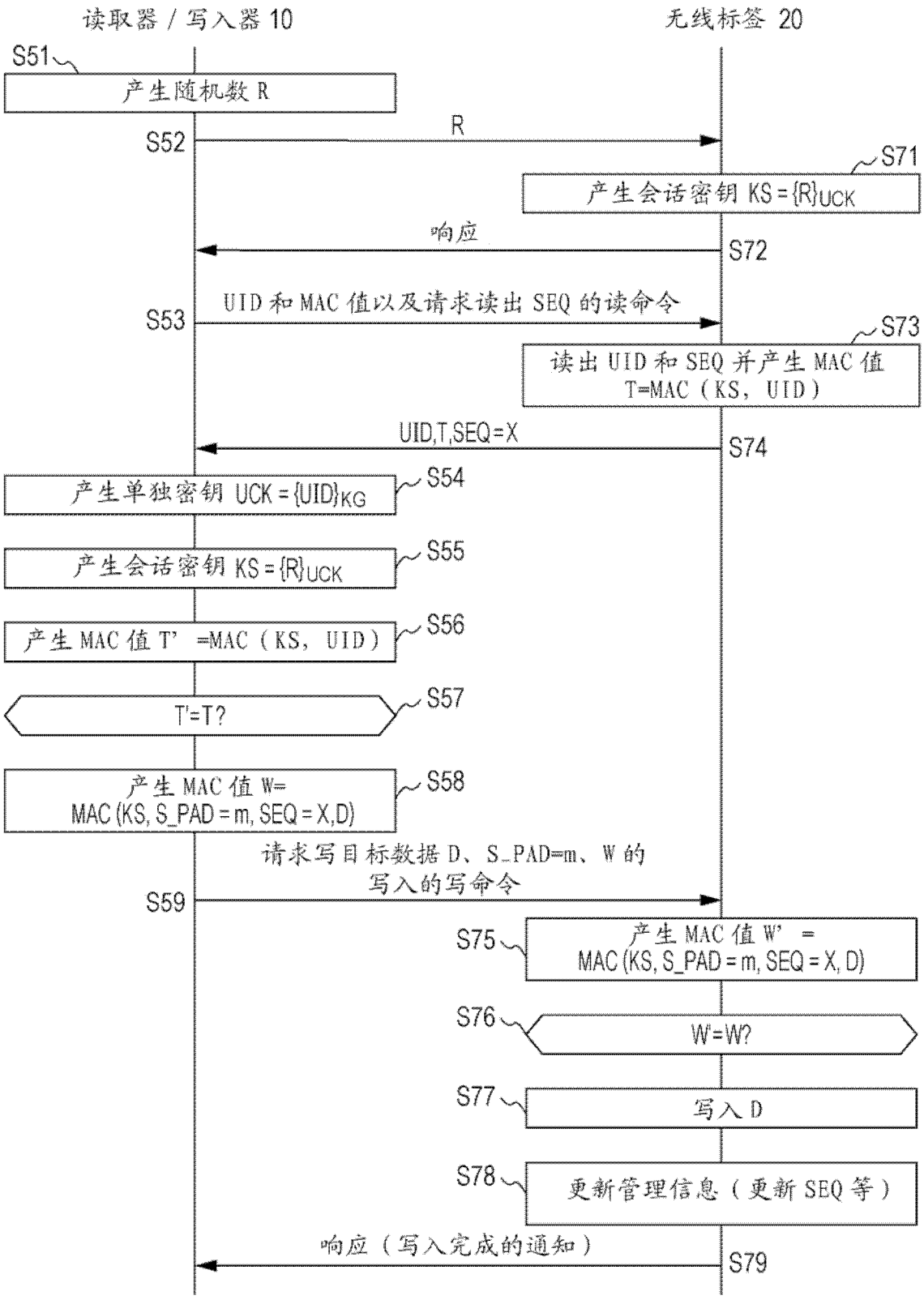

读取器 / 写入器 10
无线标签 20
S51
产生随机数 R
R
S52
S71
产生会话密钥 KS = {R}UCK
响应
S72
UID 和 MAC 值以及请求读出 SEQ 的读命令
S53
S73
读出 UID 和 SEQ 并产生 MAC 值
T=MAC（KS，UID）
UID,T,SEQ=X
S74
产生单独密钥 UCK = {UID}KG
S54
产生会话密钥 KS = {R}UCK
S55
产生 MAC 值 T' =MAC（KS，UID）
S56
T'=T?
S57
产生 MAC 值 W=
MAC (KS, S_PAD = m, SEQ = X,D)
S58
请求写目标数据 D、S_PAD=m、W 的
写入的写命令
S59
S75
产生 MAC 值 W' =
MAC (KS, S_PAD = m, SEQ = X, D)
S76
W'=W?
S77
写入 D
S78
更新管理信息（更新 SEQ 等）
响应（写入完成的通知）
S79

图 7

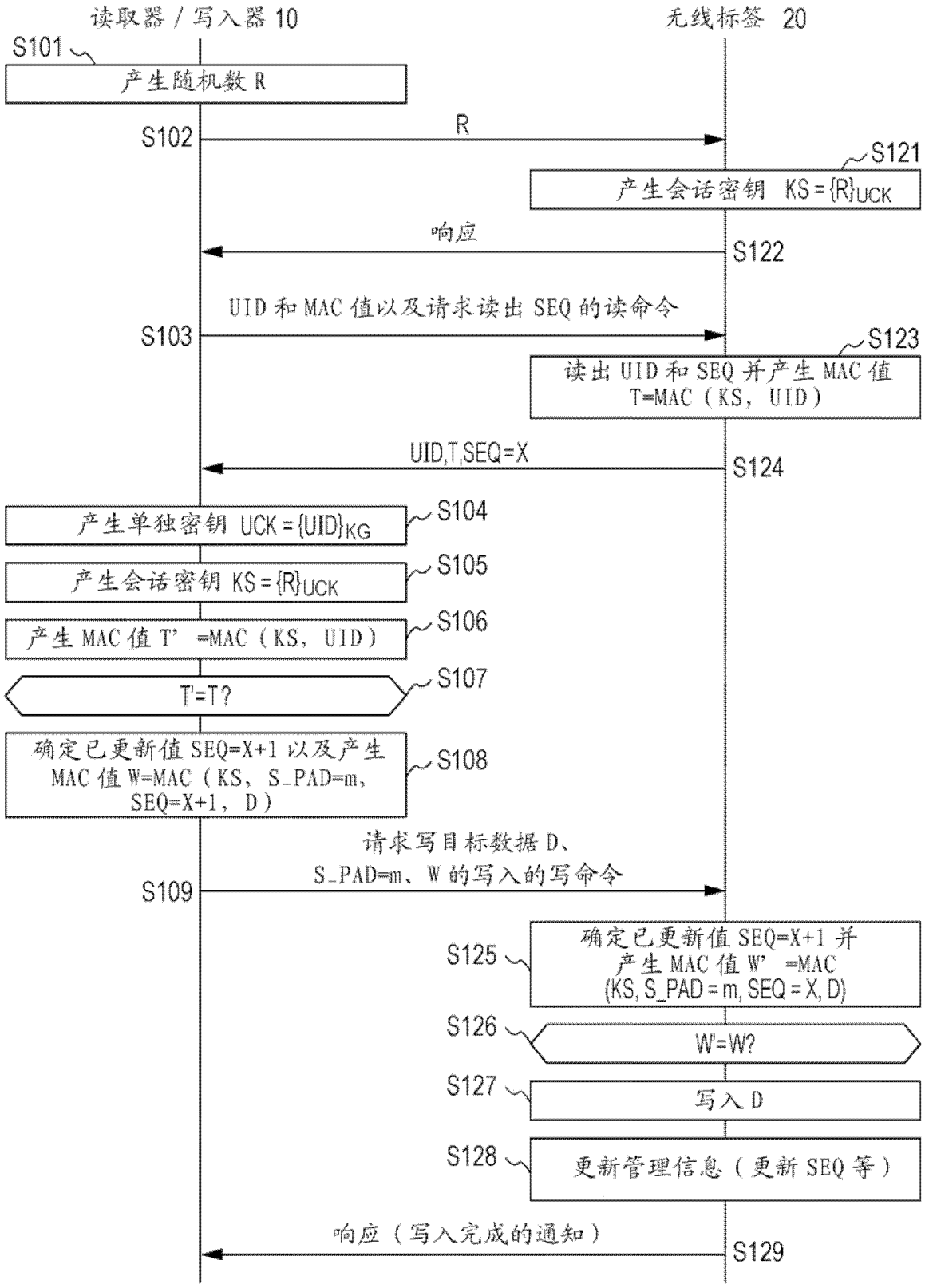

读取器 / 写入器 10
无线标签 20
S101
产生随机数 R
S102
R
S121
产生会话密钥 KS = {R}UCK
响应
S122
UID 和 MAC 值以及请求读出 SEQ 的读命令
S103
S123
读出 UID 和 SEQ 并产生 MAC 值
T=MAC（KS，UID）
UID,T,SEQ=X
S124
产生单独密钥 UCK = {UID}KG
S104
产生会话密钥 KS = {R}UCK
S105
产生 MAC 值 T' =MAC（KS，UID）
S106
T'=T?
S107
确定已更新值 SEQ=X+1 以及产生
MAC 值 W=MAC（KS，S_PAD=m，
SEQ=X+1，D）
S108
请求写目标数据 D、
S_PAD=m、W 的写入的写命令
S109
S125
确定已更新值 SEQ=X+1 并
产生 MAC 值 W' =MAC
(KS, S_PAD = m, SEQ = X, D)
S126
W'=W?
S127
写入 D
S128
更新管理信息（更新 SEQ 等）
响应（写入完成的通知）
S129

图 8

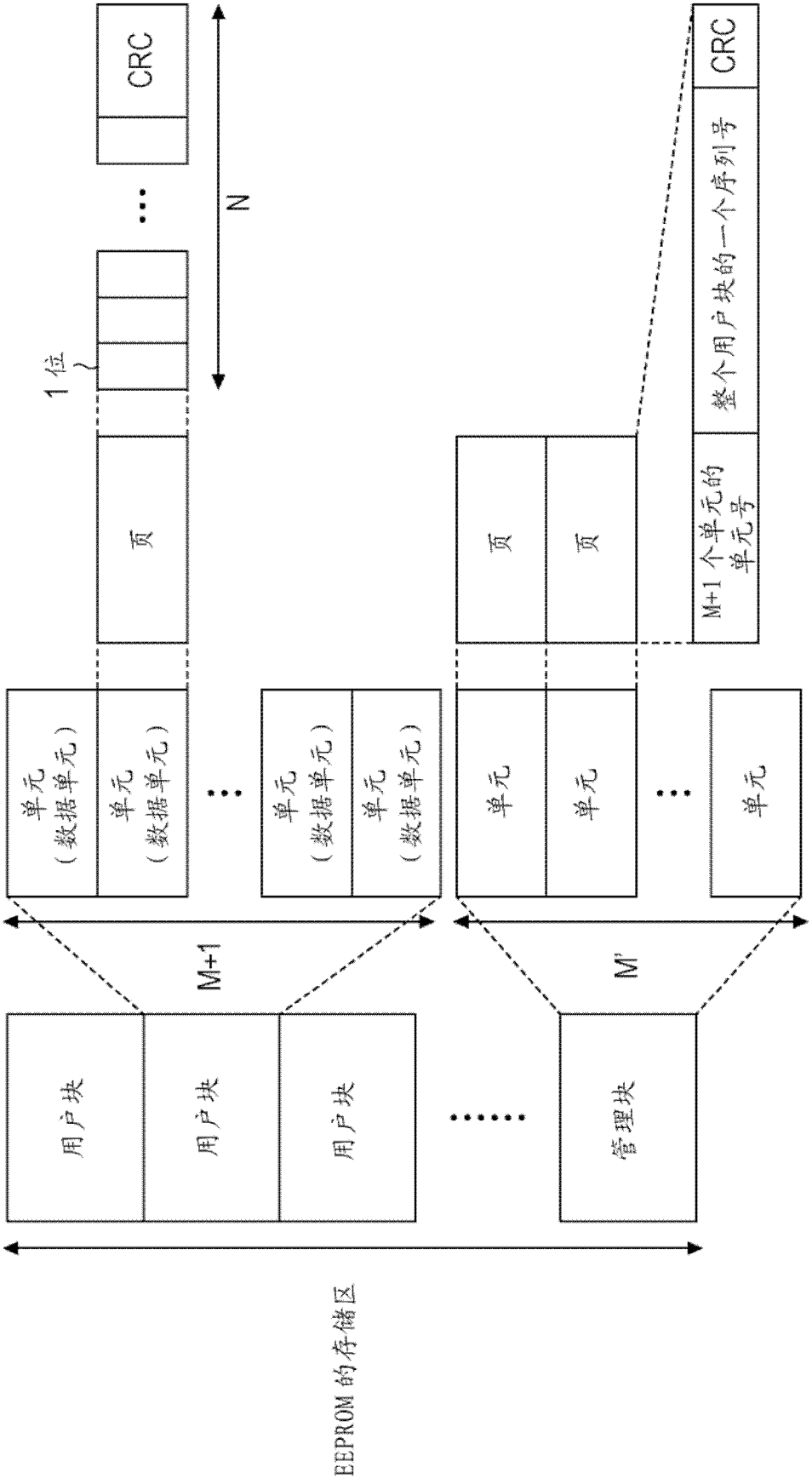

EEPROM 的存储区
用户块
用户块
用户块
管理块
M+1
M'
单元（数据单元）
单元（数据单元）
单元（数据单元）
单元（数据单元）
单元
单元
单元
页
页
页
1 位
N
CRC
CRC
整个用户块的一个序列号
M+1 个单元的单元号

图 9