(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 103136552 B
(45)授权公告日 2016.02.24

(21)申请号 201110397649.8

(22)申请日 2011.12.02

(73)专利权人 中国航天科工集团第二研究院七0六所
地址 100854 北京市海淀区永定路51号西工业区96号楼
专利权人 北京市爱威电子技术公司

(72)发明人 蒋遂平

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 梁挥 祁建国

(51)Int.Cl.
G06K 17/00(2006.01)
G06K 19/073(2006.01)

(56)对比文件
CN 102063601 A,2011.05.18,
CN 102110233 A,2011.06.29,
WO 2009065317 A1,2009.05.28,
CN 201820283 U,2011.05.04,

审查员 楚丹丹

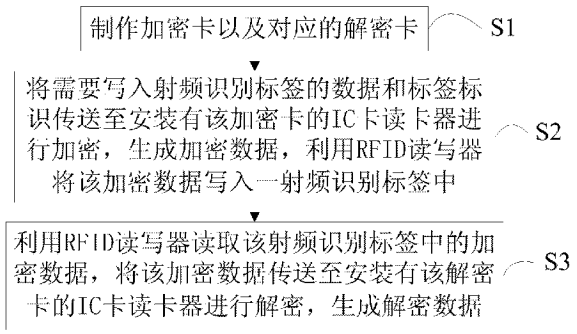
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种保护射频识别标签数据的方法及系统

(57)摘要

本发明公开了一种保护射频识别标签数据的方法及系统，该方法包括：制作加密卡以及对应的解密卡；将需要写入射频识别标签的数据和标签标识传送至安装有该加密卡的IC卡读卡器进行加密，生成加密数据，利用RFID读写器将该加密数据写入一射频识别标签中；利用RFID读写器读取该射频识别标签中的该加密数据，将该加密数据传送至安装有该解密卡的IC卡读卡器进行解密，生成解密数据。本发明有效保护了射频识别标签内数据的安全性。本发明利用IC卡技术，对现有的RFID应用系统的改动较小，可兼容性较高。在原有RFID系统的基础上，增加的成本只是IC卡系统的成本，其成本较为低廉。



CN 103136552 B

1. 一种保护射频识别标签数据的系统，其特征在于，包括：

安装有密钥管理软件系统的预处理计算机，与一第一 IC 卡读卡器相连接以制作加密卡以及对应的解密卡；

安装有标签发行软件系统的 RFID 标签发行设备，与一第二 IC 卡读卡器以及一第一 RFID 读写器相连接，该第二 IC 卡读卡器安装有该加密卡，该标签发行软件系统将需要写入射频识别标签的数据和标签标识传送至该第二 IC 卡读卡器进行加密，生成加密数据，并利用该第一 RFID 读写器将该加密数据写入一射频识别标签中；

安装有标签读取软件系统的 RFID 标签读取设备，与一第三 IC 卡读卡器以及一第二 RFID 读写器相连接，该第三 IC 卡读卡器安装有该解密卡，该标签读取软件系统利用该第二 RFID 读写器读取该射频识别标签中的该加密数据，将该加密数据传送至该第三 IC 卡读卡器进行解密，生成解密数据。

2. 如权利要求 1 所述的系统，其特征在于，该第二 IC 卡读卡器的加密卡中存储有加密密钥，该第二 IC 卡读卡器的加密卡用于利用该加密密钥对该标签标识进行加密，生成新加密密钥并利用该新加密密钥对该需要写入射频识别标签的数据进行加密生成该加密数据。

3. 如权利要求 1 或 2 所述的系统，其特征在于，该第三 IC 卡读卡器的解密卡中存储有解密密钥，该第三 IC 卡读卡器的解密卡用于利用该解密密钥对该标签标识进行加密，生成新解密密钥，利用该新解密密钥对该加密数据进行解密，生成该解密数据。

4. 如权利要求 1 所述的系统，其特征在于，该第一 IC 卡读卡器用于接受该密钥管理软件系统的控制而将一 PSAM 卡制作成 A 码单卡，将另一 PSAM 卡制作成 B 码单卡，进而根据该 A 码单卡和该 B 码单卡制作一主密钥卡，并根据该主密钥卡分别制作该加密卡和该解密卡。

5. 如权利要求 3 所述的系统，其特征在于，该加密密钥的长度为 128 位，该解密密钥的长度为 128 位。

6. 一种应用于如权利要求 1-5 中任一所述的保护射频识别标签数据的系统的保护射频识别标签数据的方法，其特征在于，包括：

预处理步骤，利用所述预处理计算机制作加密卡以及对应的解密卡；

写入步骤，该系统将需要写入射频识别标签的数据和标签标识传送至安装有该加密卡的该第二 IC 卡读卡器进行加密，生成加密数据，利用该第一 RFID 读写器将该加密数据写入一射频识别标签中；

读取步骤，利用该第二 RFID 读写器读取该射频识别标签中的该加密数据，将该加密数据传送至安装有该解密卡的该第三 IC 卡读卡器进行解密，生成解密数据。

7. 如权利要求 6 所述的方法，其特征在于，该写入步骤进一步包括：

该加密卡利用其所存储的加密密钥对该标签标识进行加密，生成新加密密钥，利用该新加密密钥对该需要写入射频识别标签的数据进行加密生成该加密数据。

8. 如权利要求 6 或 7 所述的方法，其特征在于，该读取步骤进一步包括：

该解密卡利用其所存储的解密密钥对该标签标识进行加密，生成新解密密钥，利用该新解密密钥对该加密数据进行解密，生成该解密数据。

9. 如权利要求 6 所述的方法，其特征在于，该预处理步骤进一步包括：

将一 PSAM 卡制作成 A 码单卡，将另一 PSAM 卡制作成 B 码单卡；

利用该 A 码单卡和该 B 码单卡制作一主密钥卡；

利用该主密钥卡分别制作该加密卡和该解密卡。

10. 如权利要求 8 所述的方法，其特征在于，该加密密钥的长度为 128 位，该解密密钥的长度为 128 位。

一种保护射频识别标签数据的方法及系统

技术领域

[0001] 本发明涉及射频识别领域，特别是涉及一种保护射频识别标签数据的方法及系统。

背景技术

[0002] RFID（射频识别）技术具有快速、远距、多目标、非视线识读物品的特点，而且无源RFID标签不需要电池供能和维护，因而被广泛应用于物流管理、车辆管理等需要跟踪物品的领域。目前，被广泛采用的超高频RFID标签是符合ISO/IEC 18000-6C标准的RFID标签。

[0003] ISO/IEC 18000-6C的RFID系统主要目的是应用于物流跟踪中的单品管理，要求能够实现快速、远距的RFID标签识别和读写；由于RFID标签用于单个物品管理，就要求RFID标签的成本低廉。这样，RFID标签的安全性比较低，利用ISO/IEC 18000-6C标准规定的强制命令集，仅能实现对RFID标签数据的写保护，不能实现对RFID标签数据的读保护，存储在RFID标签中的数据可以被任何持有符合ISO/IEC 18000-6C标准的RFID读写器读取，RFID标签中存储的数据没有秘密可言。

[0004] 目前解决RFID标签数据读保护的一个方法是，设计和制造具有数据读保护能力的RFID标签。这样的专用RFID标签符合ISO/IEC 18000-6C标准，但具有专有命令集。由于专用RFID标签由不同的厂商设计和制造，专有命令集可能不相同，并需要设计和制造相应的RFID读写器，这种方法限制了RFID应用系统中标签和读写器的选择范围，提高了RFID应用的成本。由于RFID标签数据的读保护是采用密码（口令）方式实现的，密码长度只有32个二进制位，并且需要通过无线电波传输，因此密码容易被窃听和破译。如果一个RFID应用系统中每个标签采用不同的密码，就需要应用系统中RFID读写设备存储大量的密码，或者读写设备与后端系统进行实时交互，根据RFID标签的唯一标识符，从后端系统获取标签的密码。因此，这种方法的可行性、安全性都比较低。

[0005] 因此，市场需要一种简单易行、成本低廉、安全性较高的RFID标签数据的保护方法，本发明正是基于这种现实需求而产生的。

发明内容

[0006] 本发明要解决的技术问题是，克服以上采用密码保护RFID标签数据的缺陷，提供一种能够对RFID标签中存储的数据进行有效保护、实施成本低廉、在中小规模的RFID应用系统中切实可行的数据保护方法，以保护RFID标签所有者的商业秘密。

[0007] 为解决上述问题，本发明公开了一种保护射频识别标签数据的方法，包括：

[0008] 预处理步骤，制作加密卡以及对应的解密卡；

[0009] 写入步骤，将需要写入射频识别标签的数据和标签标识传送至安装有该加密卡的IC卡读卡器进行加密，生成加密数据，利用RFID读写器将该加密数据写入一射频识别标签中；

[0010] 读取步骤，利用RFID读写器读取该射频识别标签中的该加密数据，将该加密数据

传送至安装有该解密卡的 IC 卡读卡器进行解密，生成解密数据。

[0011] 该写入步骤进一步包括：该加密卡利用其所存储的加密密钥对该标签标识进行加密，生成新加密密钥，利用该新加密密钥对该需要写入射频识别标签的数据进行加密生成该加密数据。

[0012] 该读取步骤进一步包括：

[0013] 该解密卡利用其所存储的解密密钥对该标签标识进行加密，生成新解密密钥，利用该新解密密钥对该加密数据进行解密，生成该解密数据。

[0014] 该预处理步骤进一步包括：将一 PSAM 卡制作成 A 码单卡，将另一 PSAM 卡制作成 B 码单卡；利用该 A 码单卡和该 B 码单卡制作一主密钥卡；利用该主密钥卡分别制作该加密卡和该解密卡。

[0015] 该加密密钥的长度为 128 位，该解密密钥的长度为 128 位。

[0016] 本发明还公开了一种保护射频识别标签数据的系统，包括：

[0017] 安装有密钥管理软件系统的预处理计算机，与一第一 IC 卡读卡器相连接以制作加密卡以及对应的解密卡；

[0018] 安装有标签发行软件系统的 RFID 标签发行设备，与一第二 IC 卡读卡器以及一第一 RFID 读写器相连接，该第二 IC 卡读卡器安装有该加密卡，该标签发行软件系统将需要写入射频识别标签的数据和标签标识传送至该第二 IC 卡读卡器进行加密，生成加密数据，并利用该第一 RFID 读写器将该加密数据写入一射频识别标签中；

[0019] 安装有标签读取软件系统的 RFID 标签读取设备，与一第三 IC 卡读卡器以及一第二 RFID 读写器相连接，该第三 IC 卡读卡器安装有该解密卡，该标签读取软件系统利用该第二 RFID 读写器读取该射频识别标签中的该加密数据，将该加密数据传送至该第三 IC 卡读卡器进行解密，生成解密数据。

[0020] 该第二 IC 卡读卡器的加密卡中存储有加密密钥，该第二 IC 卡读卡器的加密卡用于利用该加密密钥对该标签标识进行加密，生成新加密密钥并利用该新加密密钥对该需要写入射频识别标签的数据进行加密生成该加密数据。

[0021] 该第三 IC 卡读卡器的解密卡中存储有解密密钥，该第三 IC 卡读卡器的解密卡用于利用该解密密钥对该标签标识进行加密，生成新解密密钥，利用该新解密密钥对该加密数据进行解密，生成该解密数据。

[0022] 该第一 IC 卡读卡器用于接受该密钥管理软件系统的控制而将一 PSAM 卡制作成 A 码单卡，将另一 PSAM 卡制作成 B 码单卡，进而根据该 A 码单卡和该 B 码单卡制作一主密钥卡，并根据该主密钥卡分别制作该加密卡和该解密卡。

[0023] 该加密密钥的长度为 128 位，该解密密钥的长度为 128 位。

[0024] 本发明的技术效果在于，由于该加密卡、解密卡的设置，有效保护了射频识别标签内数据的安全性。本发明利用的是 IC 卡技术，对现有的 RFID 应用系统的改动较小，可兼容性较高。在原有 RFID 系统的基础上，增加的成本只是 IC 卡系统的成本，其成本低廉。

[0025] 另外，在本发明中，该加密密钥的长度可为 128 位，该解密密钥的长度可为 128 位，远大于现有密码的 32 位，安全性较高。本发明中加密和解密所使用的密钥也不需要通过无线电波传输，避免了通过无线电波泄密。与现有技术中的密码保护方式相比，本发明加大了破译存储在 RFID 标签数据的难度，能有效保护存储在 RFID 标签数据中的商业秘密，扩大

RFID 系统的应用范围。

[0026] 同时，本发明扩大了选择 RFID 系统的范围，允许选择任何符合 RFID 标准的 RFID 读写器和标签，不再受专用 RFID 系统的制约。

附图说明

[0027] 图 1 所示为本发明的保护射频识别标签数据的系统的结构示意图；

[0028] 图 2 所示为本发明的保护射频识别标签数据的方法的流程图。

具体实施方式

[0029] 如图 1 所示为本发明的保护射频识别标签数据的系统的结构示意图。保护射频识别标签数据的系统 100 包括预处理计算机 10、RFID 标签发行设备 20、RFID 标签读取设备 30、IC 卡读卡器 (41、42、43)、RFID 读写器 (51、52)、至少一射频识别标签 (RFID 标签)6。

[0030] 其中，IC 卡读卡器 41 与该预处理计算机 10 连接。IC 卡读卡器 42 与该 RFID 标签发行设备 20 连接，RFID 读写器 51 也与 RFID 标签发行设备 20 连接。IC 卡读卡器 43 与该 RFID 标签读取设备 30 连接，RFID 读写器 52 也与该 RFID 标签读取设备 30 连接。

[0031] 射频识别标签 6 可应用于该 RFID 读写器 51、52 中，该 RFID 读写器 51、52 用于读写存储在射频识别标签 6 上的数据。

[0032] 该预处理计算机 10 中安装运行一密钥管理软件系统 11。该密钥管理软件系统 11 用于制作加密卡 D、解密卡 E，该加密卡 D 中存储有加密密钥 D1，该解密卡 E 中存储有解密密钥 E1。

[0033] 该 RFID 标签发行设备 20 中安装并运行一标签发行软件系统 21，标签发行软件系统 21 借助于该 IC 卡读卡器 42 控制针对射频识别标签 6 的数据加密存入过程。该 RFID 标签读取设备 30 中安装并运行一标签读取软件系统 31，该标签读取软件系统 31 借助该 IC 卡读卡器 43 控制针对射频识别标签 6 的数据解密读出过程。

[0034] 以下结合图 1 所记载的内容，详细说明本发明的技术方案。

[0035] 为了提供一种实施成本低廉的技术方案以实现对 RFID 标签中存储的数据进行有效保护，本发明将常用的 RFID 技术和 IC 卡技术结合，利用 IC 卡的加密和解密功能，对存储在 RFID 标签中的数据进行加密和解密，以确保数据安全性。

[0036] 本发明通过该预处理计算机 10 及该密钥管理软件系统 11，制作出加密卡 D 以及与该加密卡 D 相对应的解密卡 E，具体制作方式容后述。

[0037] 在产品生产方一侧设置有该 RFID 标签发行设备 20，用于为各种产品设置射频识别标签，通常通过黏贴的方式设置该射频识别标签。将加密卡 D 安装在该 IC 卡读卡器 42 中。

[0038] 首先，为射频识别标签写入数据。本发明利用 RFID 技术和 IC 卡技术的结合，为射频识别标签写入经过 IC 卡加密的数据。

[0039] 标签发行软件系统 21 将需要写入射频识别标签 6 的产品数据和能够唯一标识该射频识别标签的标签标识传送至该 IC 卡读卡器 42，通过该加密卡 D 进行加密，以生成加密数据。在得到该加密数据后，利用该 RFID 读写器 51 将该加密数据写入射频识别标签 6 中。随后将射频识别标签 6 设置在产品上，射频识别标签 6 随产品流向各地。

[0040] 在一具体实施例中，可通过如下方式完成加密。标签发行软件系统 21 将需要写入射频识别标签 6 的产品数据和能够唯一标识该射频识别标签的标签标识传送至该 IC 卡读卡器 42，该 IC 卡读卡器 42 利用加密卡 D 的加密密钥 D1 对该标签标识进行加密以生成新加密密钥 D2，并且该 IC 卡读卡器 42 还利用该新加密密钥 D2 对该需要写入射频识别标签 6 的产品数据进行加密，从而生成该加密数据。该加密数据包括能够唯一标识该射频识别标签的标签标识以及对产品数据进行加密后的数据。

[0041] 随后，在商超结算等需要识别产品信息的场合，设置该 RFID 标签读取设备 30，解密卡 E 安装在与该 RFID 标签读取设备 30 连接的 IC 卡读卡器 43 中。该标签读取软件系统利用该 RFID 读写器 52 读取一产品的该射频识别标签 6 中的该加密数据，将该加密数据传送至该 IC 卡读卡器 43 进行解密，生成解密数据。该标签读取软件系统可将该解密数据显示在屏幕上以供阅览。

[0042] 在一具体实施例中，可通过如下方式完成解密。标签读取软件系统 31 控制该 RFID 读写器 52 读取一产品的该射频识别标签 6 中的该加密数据，并将该加密数据发送至该 IC 卡读卡器 43。IC 卡读卡器 43 利用该解密卡 E 的解密密钥 E1 对该标签标识进行加密，生成新解密密钥 E2，IC 卡读卡器 43 利用该新解密密钥 E2 对该加密数据进行解密，生成该解密数据。

[0043] 由于该加密卡、解密卡的设置，使得在射频识别标签被写入数据后，如果需读取该射频识别标签内的数据，则必须拥有该解密卡，否则，利用通用的 RFID 读写器是无法获得该射频识别标签内的数据的，进而有效保护了射频识别标签内数据的安全性。而解密卡可由特定部门利用相关审核手续对申请者资质进行审核，通过则进行发放，从而控制能够拥有解密卡的单位或个人。本发明利用的是 IC 卡技术，对现有的 RFID 应用系统的改动较小，可兼容性较高。在原有 RFID 系统的基础上，增加的成本只是 IC 卡系统的成本，其成本低廉。

[0044] 另外，在本发明中，该加密密钥的长度可为 128 位，该解密密钥的长度可为 128 位，远大于现有密码的 32 位，安全性较高。本发明中加密和解密所使用的密钥也不需要通过无线电波传输，避免了通过无线电波泄密。与现有技术中的密码保护方式相比，本发明加大了破译存储在 RFID 标签数据的难度，能有效保护存储在 RFID 标签数据中的商业秘密，扩大 RFID 系统的应用范围。

[0045] 同时，本发明扩大了选择 RFID 系统的范围，允许选择任何符合 RFID 标准的 RFID 读写器和标签，不再受专用 RFID 系统的制约。

[0046] 接下来说明该加密卡 D 和解密卡 E 的制作过程。

[0047] 该预处理计算机 10 可为禁止接入互联网的专用计算机，同时配备了至少 5 张具有 PSAM（消费安全访问模块）功能的 IC 卡 (PSAM 卡)，该密钥管理软件系统 11 控制该 IC 卡读卡器 41 将第一张 IC 卡制作成 A 码单卡 (A)，将第二张 IC 卡制作为 B 码单卡 (B)。该 A 码单卡包含根密钥 A 部分和使用 A 码单卡的密码。该 B 码单卡包含根密钥 B 部分和使用 B 码单卡的密码。该密钥管理软件系统 11 进一步控制该 IC 卡读卡器 41 参照该 A 码单卡和 B 码单卡，将第三张 IC 卡制作成为一主密钥卡 C。该主密钥卡 C 上存储有根密钥、分散参数和使用主密钥卡的密码。该密钥管理软件系统 11 进一步控制该 IC 卡读卡器 41 将一张或多张该 IC 卡制作成加密卡 D，该加密卡 D 上存储有加密 RFID 标签 6 上数据的加密密钥。该密钥管理软件系统 11 进一步控制该 IC 卡读卡器 41 将一张或多张该 IC 卡制作成解密卡 E，

该解密卡 E 上存储有解密 RFID 标签 6 上数据的解密密钥。

[0048] 其中，A 码单卡、B 码单卡、主密钥卡 C、加密卡 D、解密卡 E 均由专人保管，防止泄密。

[0049] 以上加密卡 D 和解密卡 E 的制作过程仅为示例说明，现有技术中的其他加、解密卡的制作方法也在本发明的公开范围内，只要加、解密卡中分别具有对应的加、解密密钥即可。

[0050] 如图 2 所示为本发明的一种保护射频识别标签数据的方法的流程图。

[0051] 预处理步骤，制作加密卡以及对应的解密卡 (S1)；

[0052] 写入步骤，将需要写入射频识别标签的数据和标签标识传送至安装有该加密卡的 IC 卡读卡器进行加密，生成加密数据，利用 RFID 读写器将该加密数据写入一射频识别标签中 (S2)；

[0053] 读取步骤，利用 RFID 读写器读取该射频识别标签中的该加密数据，将该加密数据传送至安装有该解密卡的 IC 卡读卡器进行解密，生成解密数据 (S3)。

[0054] 该写入步骤进一步包括：该加密卡利用其所存储的加密密钥对该标签标识进行加密，生成新加密密钥，利用该新加密密钥对该需要写入射频识别标签的数据进行加密生成该加密数据。

[0055] 该读取步骤进一步包括：该解密卡利用其所存储的解密密钥对该标签标识进行加密，生成新解密密钥，利用该新解密密钥对该加密数据进行解密，生成该解密数据。

[0056] 该预处理步骤进一步包括：将一 PSAM 卡制作成 A 码单卡，将另一 PSAM 卡制作成 B 码单卡；利用该 A 码单卡和该 B 码单卡制作一主密钥卡；利用该主密钥卡分别制作该加密卡和该解密卡。

[0057] 以上描述仅为本发明的具体实施方式，在不偏离本发明构思的前提下，对本发明的简单修改和替换应包含在本发明的技术构思之内。

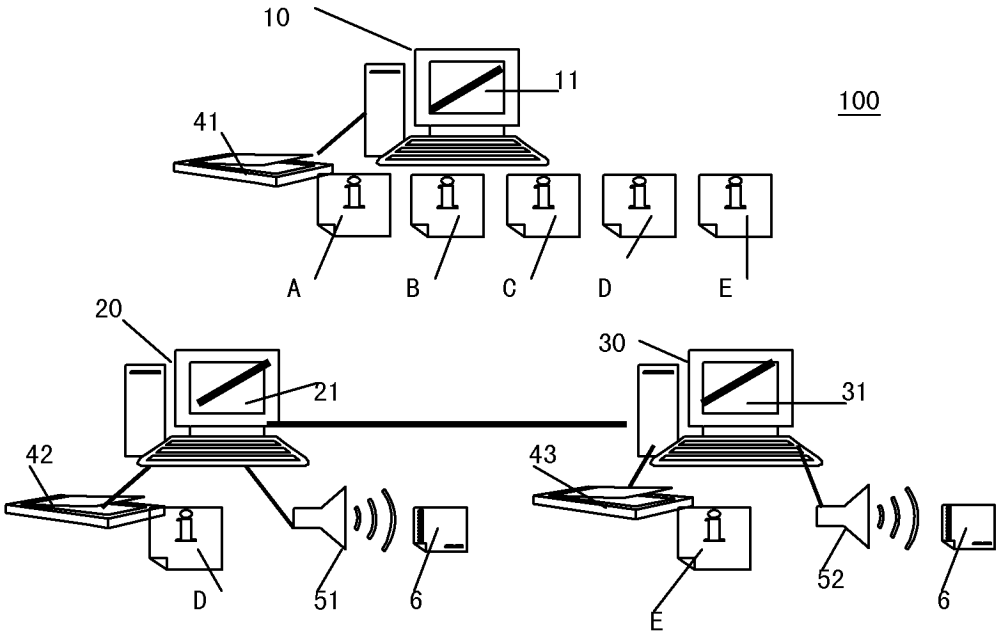

10
11
100
41
A
B
C
D
E
20
21
30
31
42
43
D
51
6
E
52
6

图 1

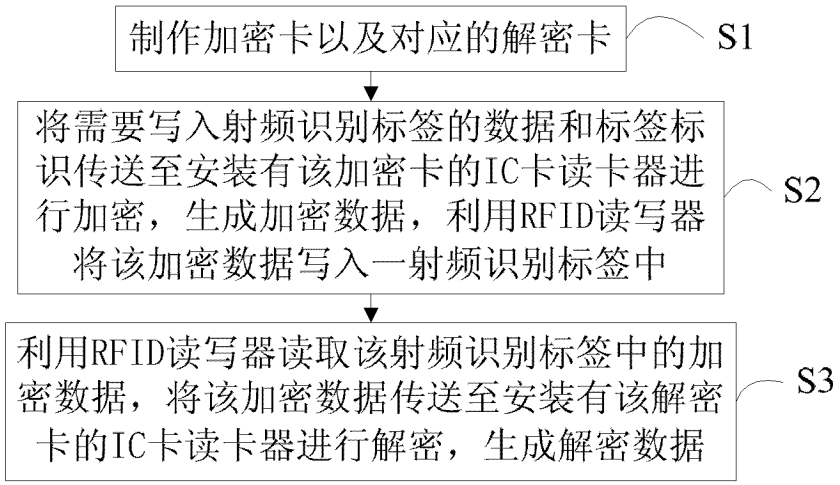

制作加密卡以及对应的解密卡
S1
将需要写入射频识别标签的数据和标签标识传送至安装有该加密卡的IC卡读卡器进行加密，生成加密数据，利用RFID读写器将该加密数据写入一射频识别标签中
S2
利用RFID读写器读取该射频识别标签中的加密数据，将该加密数据传送至安装有该解密卡的IC卡读卡器进行解密，生成解密数据
S3

图 2