(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295449 A
(43)申请公布日 2017.01.04

(21)申请号 201610676046.4

(22)申请日 2016.08.16

(71)申请人 广东工业大学
地址 510062 广东省广州市越秀区东风东路729号大院

(72)发明人 李倩 苏庆 何凡

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 杨炳财 屈慧丽

(51)Int.Cl.
G06K 7/10(2006.01)
H04L 9/32(2006.01)

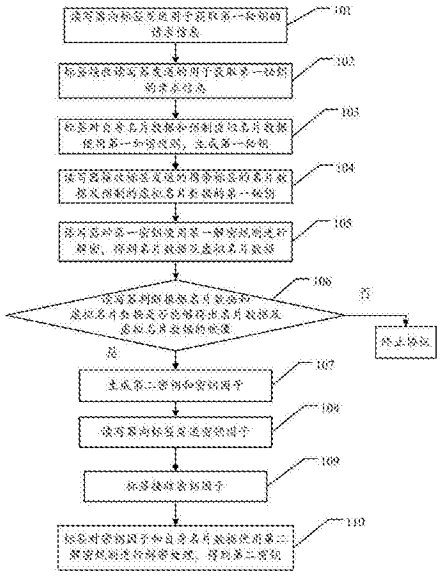
权利要求书4页 说明书11页 附图3页

(54)发明名称

一种认证方法，系统，读写器和标签

(57)摘要

本发明实施例公开了一种认证方法，系统，读写器和标签，提出了一种基于假名标识的RFID系统密钥无线生成方案，实现计算量少、标签成本低、安全性高的RFID系统密钥无线生成。本发明的一种认证方法，包括：读写器向标签发送用于获取第一密钥的请求信息；标签接收读写器发送的用于获取第一密钥的请求信息；标签对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；读写器接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；读写器对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；读写器判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像。



CN 106295449 A

1.一种认证方法,其特征在于,包括:

读写器向标签发送用于获取第一密钥的请求信息;

标签接收所述读写器发送的用于获取第一密钥的请求信息;

标签对自身名片数据和预制虚拟名片数据使用第一加密规则,生成第一密钥;

读写器接收所述标签发送的携带所述标签的名片数据及预制的虚拟名片数据的第一密钥;

所述读写器对所述第一密钥使用第一解密规则进行解密,得到名片数据及虚拟名片数据;

读写器判断根据所述名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像;

若能够得出名片数据及虚拟名片数据的映像,则生成第二密钥和密钥因子,其中所述密钥因子和所述第二密钥之间满足预置对应关系,且所述标签根据所述对应关系、所述密钥因子和自身名片数据能够得出所述第二密钥;

所述读写器向所述标签发送所述密钥因子;

所述标签接收所述密钥因子;

所述标签对所述密钥因子和自身名片数据使用第二解密规则进行解密处理,得到所述第二密钥;

其中,所述名片数据记作ID;

所述虚拟名片数据记作IDS;

所述第一密钥记作X;

所述第二密钥记作k;

所述密钥因子记作k_i。

2.根据权利要求1所述的认证方法,其特征在于,

所述生成第二密钥和密钥因子步骤包括:

生成所述第二密钥包括:

生成第一随机数值和第二随机数值;

根据所述第一随机数和所述第二随机数值使用第二加密规则,得到第二密钥;

生成所述密钥因子包括:

读写器对所述第一随机数值和所述虚拟名片数据,使用第一编译规则,生成第一认证信息;

读写器对所述第二随机数值和所述虚拟名片数据,使用第二编译规则,生成第二认证信息;

读写器对所述第一随机数值和所述第二随机数值,使用第三编译规则,生成第三认证信息;

所述标签对所述密钥因子和自身名片数据进行解密处理,得到所述第二密钥步骤包括:

标签接收所述读写器发送的第一认证信息、第二认证信息和第三认证信息;

标签对所述第一验证信息和虚拟名片数据,使用第一逆编译规则,生成准第一随机数值;

标签对所述第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

标签根据所述准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

标签判断所述第三认证信息与所述准第三认证信息是否一致；

若是，则对所述准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥；

若否，则终止协议；

其中，所述第一随机数值记作r1；

所述第二随机数值记作r2；

所述第一认证信息记作A；

所述第二认证信息记作B；

所述第三认证信息记作C。

3.根据权利要求2所述的认证方法，其特征在于，

所述第一加密规则包括：$X=ID\oplus IDS$；

所述第一编译规则包括：$A=r1\oplus IDS$；

所述第一逆编译规则包括：$r1=A\oplus IDS$；

所述第二编译规则包括：$B=r2\oplus IDS$；

所述第二逆编译规则包括：$r2=B\oplus IDS$；

所述第三编译规则包括：$C=(r1\oplus r2)>>l$；

所述第二加密规则包括：$k_i=r1\oplus r2$或者$k_i=r1\oplus r2\oplus IDS$。

4.根据权利要求1所述的认证方法，其特征在于，

所述生成第二密钥和密钥因子步骤包括：

生成所述第二密钥包括：

对所述名片数据使用第三加密规则，生成第二密钥；

所述密钥因子与所述第二密钥之间的对应关系为：$k_i=k\oplus IDS_i$；

其中，角标i为相应标签编号数。

5.一种应用如权利要求1至4中任一项所述认证方法的读写器，其特征在于，包括：

第一获取单元，用于向标签发送用于获取第一密钥的请求信息；

第一接收单元，用于接收所述标签发送的携带所述标签的名片数据及预制的虚拟名片数据的第一密钥；

第一解密单元，用于对所述第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

第一判断单元，用于判断根据所述名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

第一生成单元，用于生成第二密钥；

第二生成单元，用于生成密钥因子；

第一发送单元，用于向所述标签发送所述密钥因子。

6.根据权利要求5所述的其特征在于，

所述第一生成单元包括：

第一生成子单元，用于生成第一随机数值；

第二生成子单元，用于生成第二随机数值；

第一加密子单元，用于根据所述第一随机数和所述第二随机数值使用第二加密规则，得到第二密钥；

所述第二生成单元包括：

第一编译子单元，用于对所述第一随机数值和所述虚拟名片数据，使用第一编译规则，生成第一认证信息；

第二编译子单元，用于对所述第二随机数值和所述虚拟名片数据，使用第二编译规则，生成第二认证信息；

第三编译子单元，用于对所述第一随机数值和所述第二随机数值，使用第三编译规则，生成第三认证信息。

7.根据权利要求5所述的其特征在于，

所述第一生成单元还包括：

第二加密子单元，用于对所述名片数据使用第三加密规则，生成第二密钥。

8.一种应用如权利要求1至4中任一项所述认证方法的标签，其特征在于，包括：

第二接收单元，用于接收所述读写器发送的用于获取第一密钥的请求信息；

第三生成单元，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

第三接收单元，用于接收所述密钥因子；

第二解密单元，用于对所述密钥因子和自身名片数据使用第二解密规则进行解密处理，得到所述第二密钥。

9.根据权利要求8所述的标签，其特征在于，

所述第二解密单元包括：

第一逆编译子单元，用于对所述第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；

第二逆编译子单元，用于对所述第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

第三逆编译子单元，用于根据所述准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

第一判断子单元，用于判断所述第三认证信息与所述准第三认证信息是否一致；

第三生成子单元，用于对所述准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥。

10.一种应用如权利要求1至4中任一项所述认证方法的认证系统，其特征在于，包括：

读写器和标签；

所述读写器包括：

第一获取单元，用于向标签发送用于获取第一密钥的请求信息；

第一接收单元，用于接收所述标签发送的携带所述标签的名片数据及预制的虚拟名片数据的第一密钥；

第一解密单元，用于对所述第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

第一判断单元，用于判断根据所述名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

第一生成单元，用于生成第二密钥；

第二生成单元，用于生成密钥因子；

第一发送单元，用于向所述标签发送所述密钥因子；

所述标签包括：

第二接收单元，用于接收所述读写器发送的用于获取第一密钥的请求信息；

第三生成单元，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

第三接收单元，用于接收所述密钥因子；

第二解密单元，用于对所述密钥因子和自身名片数据使用第二解密规则进行解密处理，得到所述第二密钥。

一种认证方法，系统，读写器和标签

技术领域

[0001] 本发明涉及信息处理领域，尤其涉及一种认证方法，系统，读写器和标签。

背景技术

[0002] RFID(Radio Frequency Identification)即无线射频识别，俗称电子标签，是一种非接触式的自动识别技术，主要用于为各个物品建立唯一的身份标识，是物联网的重要支持技术。具有耐磨损，非接触，体积小型化等优点，广泛应用于物流、身份识别、交通运输、防伪等各个领域。RFID系统一般由3部分组成：标签、读写器和后端数据库。

[0003] 密钥生成是指利用一个交互式协议构造一个共享密钥的过程。密钥用于在两个不同实体之间建立机密的通信通道或提供数据完整性，保证协议的安全进行。在RFID标签上安全生成密钥是非常具有挑战性的。首先，如果是制造商在标签出厂之前就预先设置好密钥，会带来密钥托管问题，在监管不当的情况下容易造成密钥信息的泄露；其次，如果是读写器以无线的方式直接将密钥写入标签，那么由于读写器和标签之间是无线通信，容易受到攻击者的攻击。攻击主要分为两类：一是被动攻击.攻击者偷偷地嗅探或窃听读写器和标签之间的通信，然后根据获得的数据进行密码分析或进行跟踪等；二是主动攻击，攻击者在读写器和标签之间作为第三人存在截获读写器和标签之间交互的数据，然后通过重放或篡改的方式发送给另一方，最终导致密钥信息被窃取；最后，由于标签的成本限制，传统的密钥协商协议不能直接应用到RFID系统中。如何在满足系统安全的需求下，设计轻量级的密钥生成协议是目前要解决的主要问题。

发明内容

[0004] 本发明的一种认证方法，系统，读写器和标签，提出了一种基于假名标识的RFID系统密钥无线生成方案，实现计算量少、标签成本低、安全性高的RFID系统密钥无线生成。

[0005] 本发明提供了一种认证方法，包括：

[0006] 读写器向标签发送用于获取第一密钥的请求信息；

[0007] 标签接收读写器发送的用于获取第一密钥的请求信息；

[0008] 标签对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

[0009] 读写器接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；

[0010] 读写器对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

[0011] 读写器判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0012] 若能够得出名片数据及虚拟名片数据的映像，则生成第二密钥和密钥因子，其中密钥因子和第二密钥之间满足预置对应关系，且标签根据对应关系、密钥因子和自身名片数据能够得出第二密钥；

[0013] 读写器向标签发送密钥因子；

[0014] 标签接收密钥因子；

[0015] 标签对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥；

[0016] 其中，名片数据记作ID；

[0017] 虚拟名片数据记作IDS；

[0018] 第一密钥记作X；

[0019] 第二密钥记作k；

[0020] 密钥因子记作k_i。

[0021] 可选的，

[0022] 生成第二密钥和密钥因子步骤包括：

[0023] 生成第二密钥包括：

[0024] 生成第一随机数值和第二随机数值；

[0025] 根据第一随机数和第二随机数值使用第二加密规则，得到第二密钥；

[0026] 生成密钥因子包括：

[0027] 读写器对第一随机数值和虚拟名片数据，使用第一编译规则，生成第一认证信息；

[0028] 读写器对第二随机数值和所述虚拟名片数据，使用第二编译规则，生成第二认证信息；

[0029] 读写器对第一随机数值和第二随机数值，使用第三编译规则，生成第三认证信息；

[0030] 标签对密钥因子和自身名片数据进行解密处理，得到第二密钥步骤包括：

[0031] 标签接收读写器发送的第一认证信息、第二认证信息和第三认证信息；

[0032] 标签对第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；

[0033] 标签对第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

[0034] 标签根据准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

[0035] 标签判断第三认证信息与所述准第三认证信息是否一致；

[0036] 若是，则对准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥；

[0037] 若否，则终止协议；

[0038] 其中，第一随机数值记作r1；

[0039] 第二随机数值记作r2；

[0040] 第一认证信息记作A；

[0041] 第二认证信息记作B；

[0042] 第三认证信息记作C。

[0043] 可选的，

[0044] 第一加密规则包括：$X=ID\oplus IDS$；

[0045] 第一编译规则包括：$A=r1\oplus IDS$；

[0046] 第一逆编译规则包括：$r1=A\oplus IDS$；

[0047] 第二编译规则包括：$B=r2\oplus IDS$；

[0048] 第二逆编译规则包括：$r2=B\oplus IDS$；

[0049] 第三编译规则包括：$C=(r1\oplus r2)>>l$；

[0050] 第二加密规则包括：$k_i=r1\oplus r2$或者$k_i=r1\oplus r2\oplus IDS$。

[0051] 可选的，

[0052] 生成第二密钥和密钥因子步骤包括：

[0053] 生成第二密钥包括：

[0054] 对名片数据使用第三加密规则，生成第二密钥；

[0055] 密钥因子与第二密钥之间的对应关系为：$k_i=k\oplus IDS_i$；

[0056] 其中，角标i为相应标签编号数。

[0057] 本发明提供的一种应用上述认证方法的读写器，包括：

[0058] 第一获取单元，用于向标签发送用于获取第一密钥的请求信息；

[0059] 第一接收单元，用于接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；

[0060] 第一解密单元，用于对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

[0061] 第一判断单元，用于判断根据名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0062] 第一生成单元，用于生成第二密钥；

[0063] 第二生成单元，用于生成密钥因子；

[0064] 第一发送单元，用于向标签发送密钥因子。

[0065] 可选的，

[0066] 第一生成单元包括：

[0067] 第一生成子单元，用于生成第一随机数值；

[0068] 第二生成子单元，用于生成第二随机数值；

[0069] 第一加密子单元，用于根据第一随机数和第二随机数值使用第二加密规则，得到第二密钥；

[0070] 第二生成单元包括：

[0071] 第一编译子单元，用于对第一随机数值和虚拟名片数据，使用第一编译规则，生成第一认证信息；

[0072] 第二编译子单元，用于对第二随机数值和虚拟名片数据，使用第二编译规则，生成第二认证信息；

[0073] 第三编译子单元，用于对第一随机数值和第二随机数值，使用第三编译规则，生成第三认证信息。

[0074] 可选的，

[0075] 第一生成单元还包括：

[0076] 第二加密子单元，用于对名片数据使用第三加密规则，生成第二密钥。

[0077] 本发明提供的一种应用上述认证方法的标签，包括：

[0078] 第二接收单元，用于接收读写器发送的用于获取第一密钥的请求信息；

[0079] 第三生成单元，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

[0080] 第三接收单元，用于接收密钥因子；

[0081] 第二解密单元，用于对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。

[0082] 可选的，

[0083] 第二解密单元包括：

[0084] 第一逆编译子单元，用于对第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；

[0085] 第二逆编译子单元，用于对第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

[0086] 第三逆编译子单元，用于根据准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

[0087] 第一判断子单元，用于判断第三认证信息与准第三认证信息是否一致；

[0088] 第三生成子单元，用于对准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥。

[0089] 本发明提供的一种应用上述认证方法的认证系统，包括：

[0090] 读写器和标签；

[0091] 读写器包括：

[0092] 第一获取单元，用于向标签发送用于获取第一密钥的请求信息；

[0093] 第一接收单元，用于接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；

[0094] 第一解密单元，用于对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

[0095] 第一判断单元，用于判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0096] 第一生成单元，用于生成第二密钥；

[0097] 第二生成单元，用于生成密钥因子；

[0098] 第一发送单元，用于向标签发送密钥因子；

[0099] 标签包括：

[0100] 第二接收单元，用于接收读写器发送的用于获取第一密钥的请求信息；

[0101] 第三生成单元，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

[0102] 第三接收单元，用于接收密钥因子；

[0103] 第二解密单元，用于对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。

[0104] 从以上技术方案可以看出，本发明实施例具有以下优点：

[0105] 读写器向标签发送用于获取第一密钥的请求信息；标签接收读写器发送的用于获取第一密钥的请求信息；标签对自身名片数据和预制虚拟名片数据使用第一加密规则，生

成第一密钥;读写器接收标签发送的携带所述标签的名片数据及预制的虚拟名片数据的第一密钥;读写器对第一密钥使用第一解密规则进行解密,得到名片数据及虚拟名片数据;读写器判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像。上述步骤是读写器与标签进行的第一次加密验证过程,读写器通过验证标签的名片数据及虚拟名片数据在本地是否保留有对应映像,来确定是否与标签继续进行通信,从而增强了安全性。使用虚拟名片数据是为了防止信息被截取后暴露其真实虚拟数据,从而进一步增强了安全性。若能够得出名片数据及虚拟名片数据的映像,则生成第二密钥和密钥因子,其中密钥因子和第二密钥之间满足预置对应关系,且标签根据对应关系、密钥因子和自身名片数据能够得出第二密钥;读写器向所述标签发送密钥因子;标签接收密钥因子;标签对密钥因子和自身名片数据使用第二解密规则进行解密处理,得到第二密钥。上述步骤为读写器与标签进行的第二次加密验证过程,可以认为多个标签均接到密钥因子,任意一个标签通过密钥因子和自身名片数据均能得到第二密钥,因此该第二密钥为共享密钥。从而读写器和标签可以再通过该共享密钥通信。

附图说明

[0106] 图1为本发明一种认证方法实施例的流程图;

[0107] 图2为本发明一种读写器实施例的流程图;

[0108] 图3为本发明一种标签实施例的流程图;

[0109] 图4为本发明一种认证系统实施例的流程图。

具体实施方式

[0110] 本发明的一种认证方法,系统,读写器和标签,提出了一种基于假名标识的RFID系统密钥无线生成方案,实现计算量少、标签成本低、安全性高的RFID系统密钥无线生成。

[0111] 为了使本技术领域的人员更好地理解本发明方案,下面结合附图1-4和具体实施方式对本发明作进一步的详细说明。

[0112] 如图1,本发明提供了一种认证方法实施例,包括:

[0113] 101、读写器向标签发送用于获取第一密钥的请求信息;

[0114] 在本实施例中,在获取密钥之前读写器需向标签发送获取第一秘钥的请求信息。

[0115] 102、标签接收读写器发送的用于获取第一密钥的请求信息;

[0116] 在本实施例中,标签接收读写器所发送的信息。

[0117] 103、标签对自身名片数据和预制虚拟名片数据使用第一加密规则,生成第一密钥;

[0118] 第一加密规则包括:$X=ID\oplus IDS$;

[0119] 在本实施例中,引用名片数据和虚拟名片数据能够防止唯一标识符的泄密。

[0120] 104、读写器接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥;

[0121] 在本实施例中,读写器接收标签发送的携带标签的名片数据如ID和虚拟名片数据如IDS的第一秘钥X。

[0122] 105、读写器对第一密钥使用第一解密规则进行解密,得到名片数据及虚拟名片数

据；

[0123] 在本实施例中，加密和解密的过程能更好的保护信息不泄露。

[0124] 106、读写器判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0125] 107、若能够得出名片数据及虚拟名片数据的映像，则生成第二密钥和密钥因子，其中密钥因子和第二密钥之间满足预置对应关系，且标签根据对应关系、密钥因子和自身名片数据能够得出第二密钥；

[0126] 在本实施例中，读写器判断根据名片数据ID和虚拟名片数据IDS是否能够得出名片数据及虚拟名片数据的映像，若能则生成第二密钥k和密钥因子k_i，若不能则终止协议。

[0127] 108、读写器向标签发送密钥因子；

[0128] 109、标签接收密钥因子；

[0129] 在本实施例中，读写器向标签发送密钥因子k_i，同时标签接收，密钥因子，为后续解密做准备。

[0130] 110、标签对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥；

[0131] 其中，名片数据记作ID；

[0132] 虚拟名片数据记作IDS；

[0133] 第一密钥记作X；

[0134] 第二密钥记作k；

[0135] 密钥因子记作k_i。

[0136] 本实施例中，读写器向标签发送用于获取第一密钥的请求信息，标签接收请求信息后，对自身名片数据ID和预制虚拟名片数据IDS使用第一加密规则，生成第一密钥X，并发送给读写器，读写器接收标签发送的X，并对X使用第一解密规则进行解密，得到名片数据ID及虚拟名片数据IDS；上述步骤是读写器与标签进行的第一次加密验证过程，使用虚拟名片数据是为了防止信息被截取后暴露其真实虚拟数据，读写器通过验证标签的名片数据ID及虚拟名片数据IDS在本地是否保留有对应映像，来确定是否与标签继续进行通信，从而增强了安全性。读写器判断根据ID和IDS是否能够得出ID及IDS的映像，若能够得出映像，则生成第二密钥k和密钥因子k_i，其中k_i和k之间满足预置对应关系，且标签根据对应关系、k_i和自身名片数据ID能够得出第二密钥k；读写器向标签发送密钥因子k_i，标签接收k_i后，对k_i和自身名片数据ID使用第二解密规则进行解密处理，得到第二密钥k。上述步骤为读写器与标签进行的第二次加密验证过程，可以认为多个标签均接到密钥因子，任意一个标签通过密钥因子和自身名片数据均能得到第二密钥，因此该第二密钥为共享密钥。从而读写器和标签可以再通过该共享密钥通信，即为读写器和标签之间建立了安全可靠的通信方法。

[0137] 下面对本发明的一种认证方法实施例做进一步说明，

[0138] 生成第二密钥和密钥因子步骤包括：

[0139] 生成第二密钥包括：

[0140] 生成第一随机数值和第二随机数值；

[0141] 根据第一随机数和第二随机数值使用第二加密规则，得到第二密钥；

[0142] 第二加密规则包括：$k_i = r1 \oplus r2$或者$k_i = r1 \oplus r2 \oplus IDS$；

[0143] 在本实施例中，读写器对第一随机数值r1和第二随机数值r2使用第二加密规则，如$k_i = r1 \oplus r2$或$k_i = r1 \oplus r2 \oplus IDS$，生成第二密钥。

[0144] 生成密钥因子包括：

[0145] 读写器对第一随机数值和虚拟名片数据，使用第一编译规则，生成第一认证信息；

[0146] 第一编译规则包括：$A = r1 \oplus IDS$；

[0147] 读写器对第二随机数值和虚拟名片数据，使用第二编译规则，生成第二认证信息；

[0148] 第二编译规则包括：$B = r2 \oplus IDS$；

[0149] 读写器对第一随机数值和第二随机数值，使用第三编译规则，生成第三认证信息；

[0150] 第三编译规则包括：$C=(r1 \oplus r2) >> l$；

[0151] 在本实施例中，对读写器生成第二密钥和密钥因子步骤进行了阐述，其中生成密钥的第二加密规则包括$k_i = r1 \oplus r2$或者$k_i = r1 \oplus r2 \oplus IDS$，$k_i = r1 \oplus r2$可用生成单个标签密钥，$k_i = r1 \oplus r2 \oplus IDS$可用于生成批量标签的密钥。

[0152] 标签对密钥因子和自身名片数据进行解密处理，得到第二密钥步骤包括：

[0153] 标签接收读写器发送的第一认证信息、第二认证信息和第三认证信息；

[0154] 第一认证信息记作A，第二认证信息记作B，第三认证信息记作C；

[0155] 标签对第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；

[0156] 第一逆编译规则包括：$r1 = A \oplus IDS$；

[0157] 标签对第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

[0158] 第二逆编译规则包括：$r2 = B \oplus IDS$；

[0159] 标签根据准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

[0160] 第三编译规则包括：$C=(r1 \oplus r2) >> l$；

[0161] 标签判断第三认证信息与准第三认证信息是否一致；

[0162] 若是，则对准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥；

[0163] 若否，则终止协议；

[0164] 在本实施例中，读写器生成第二密钥的同时，标签利用认证信息、随机数值、虚拟名片数据及对应的编译规则生成准认证信息，若第三认证信息与准第三认证信息一致则继续对准第一随机数值和准第二随机数值使用第二加密规则生成第二密钥，否则终止协议。即整个认证系统采用异或、移位运算，降低了标签成本与计算量，且对通信信息进行加密传输，在实现双向认证的同时保证协议的安全性。

[0165] 其中，第一随机数值记作r1；

[0166] 第二随机数值记作r2；

[0167] 第一认证信息记作A；

[0168] 第二认证信息记作B；

[0169] 第三认证信息记作C。

[0170] 本实施例中，给出了读写器生成第二密钥和密钥因子步骤的一种方法，根据标签数量的不同选择相应的加密规则，如$k_i = r1 \oplus r2$或者$k_i = r1 \oplus r2 \oplus IDS$。另一方面，读写器分别对第一随机数值、第二随机数值和虚拟名片数据采取两两编译的规则，分别生成第一认证信息、第二认证信息和第三认证信息，并将上述认证信息发送给标签，标签根据所得认证信息进行解密处理，即采取逆编译规则，生成准第三认证信息，并判断第三认证信息与准第三认证信息是否一致，若第三认证信息与准第三认证信息一致则继续对准第一随机数值和准第二随机数值使用第二加密规则生成第二密钥，否则终止协议。整个认证系统采用异或、移位运算，降低了标签成本与计算量，且对通信信息进行加密传输，在实现双向认证的同时保证协议的安全性。

[0171] 下面对本发明的一种认证方法实施例做进一步说明，

[0172] 生成第二密钥和密钥因子步骤包括：

[0173] 生成第二密钥包括：

[0174] 对名片数据使用第三加密规则，生成第二密钥；

[0175] 密钥因子与第二密钥之间的对应关系为：$k_i = k \oplus IDS_i$；

[0176] 其中，角标i为相应标签编号数。

[0177] 本实施例中，密钥因子与第二密钥之间的对应关系为：$k_i = k \oplus IDS_i$，此方法既可以用于单个标签秘钥的生成、批量标签秘钥的生成和群组标签密钥的生成，具有应用范围广，且计算量少的优势。

[0178] 如图2，本发明提供的一种应用上述认证方法的读写器实施例，包括：

[0179] 第一获取单元201，用于向标签发送用于获取第一密钥的请求信息；

[0180] 第一接收单元202，用于接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；

[0181] 第一解密单元203，用于对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

[0182] 第一判断单元204，用于判断根据名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0183] 第一生成单元205，用于生成第二密钥；

[0184] 第二生成单元206，用于生成密钥因子；

[0185] 第一发送单元207，用于向标签发送所述密钥因子。

[0186] 本实施例中，第一获取单元201向标签发送用于获取第一密钥的请求信息；第一接收单元202接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；第一解密单元203对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；第一判断单元204判断根据名片数据和所述虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；第一生成单元205生成第二密钥；第二生成单元206生成密钥因子；第一发送单元207向标签发送密钥因子。读写器生成的第二密钥与标签生成的第二密钥为共享密钥，安全性高，且采用简单的运算降低计算量。

[0187] 下面对本发明提供的一种应用上述认证方法的读写器实施例做进一步说明，

[0188] 第一生成单元包括：

[0189] 第一生成子单元，用于生成第一随机数值；

[0190] 第二生成子单元，用于生成第二随机数值；

[0191] 第一加密子单元，用于根据第一随机数和第二随机数值使用第二加密规则，得到第二密钥；

[0192] 第二生成单元包括：

[0193] 第一编译子单元，用于对第一随机数值和虚拟名片数据，使用第一编译规则，生成第一认证信息；

[0194] 第二编译子单元，用于对第二随机数值和虚拟名片数据，使用第二编译规则，生成第二认证信息；

[0195] 第三编译子单元，用于对第一随机数值和第二随机数值，使用第三编译规则，生成第三认证信息。

[0196] 本实施例中，第一生成单元包括：第一生成子单元生成第一随机数值；第二生成子单元生成第二随机数值；第一加密子单元根据第一随机数和第二随机数值使用第二加密规则，得到第二密钥；读写器通过上述单元实现生成第二密钥。第二生成单元包括：第一编译子单元对第一随机数值和虚拟名片数据，使用第一编译规则，生成第一认证信息；第二编译子单元对第二随机数值和虚拟名片数据，使用第二编译规则，生成第二认证信息；第三编译子单元对第一随机数值和第二随机数值，使用第三编译规则，生成第三认证信息。读写器通过上述单元生成第一认证信息、第二认证信息和第三认证信息。

[0197] 下面对本发明提供的一种应用上述认证方法的读写器实施例做进一步说明，

[0198] 第一生成单元还包括：第二加密子单元，用于对名片数据使用第三加密规则，生成第二密钥。

[0199] 本实施例中，读写器的第一生成单元中的第二加密子单元能够对名片数据使用第三加密规则，生成第二密钥。第二密钥作为与标签的共享密钥，实现安全、可行的RFID密钥无线生成系统。

[0200] 如图3，本发明提供的一种应用上述认证方法的标签实施例，包括：

[0201] 第二接收单元301，用于接收读写器发送的用于获取第一密钥的请求信息；

[0202] 第三生成单元302，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

[0203] 第三接收单元303，用于接收密钥因子；

[0204] 第二解密单元304，用于对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。

[0205] 本实施例中，标签的第二接收单元301接收读写器发送的用于获取第一密钥的请求信息后，第三生成单元302对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；第三接收单元303接收密钥因子；第二解密单元304对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。此处标签生成的第二密钥与前述读写器生成的第二密钥为共享密钥，采用简单算法可以降低标签成本和计算量。

[0206] 下面对本发明提供的一种应用上述认证方法的标签实施例做进一步说明，

[0207] 第二解密单元包括：

[0208] 第一逆编译子单元，用于对第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；

[0209] 第二逆编译子单元，用于对第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；

[0210] 第三逆编译子单元，用于根据准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；

[0211] 第一判断子单元，用于判断第三认证信息与准第三认证信息是否一致；

[0212] 第三生成子单元，用于对准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥。

[0213] 本实施例中，标签的第二解密单元包括：第一逆编译子单元对第一验证信息和虚拟名片数据，使用第一逆编译规则，生成准第一随机数值；第二逆编译子单元对第二验证信息和虚拟名片数据，使用第二逆编译规则，生成准第二随机数值；第三逆编译子单元根据准第一随机数值和准第二随机数值使用第三编译规则，生成准第三认证信息；第一判断子单元判断第三认证信息与准第三认证信息是否一致；第三生成子单元对准第一随机数值和准第二随机数值使用第二加密规则，生成第二密钥。如上，减少了标签生成第二密钥的计算量，同时降低了标签的成本。

[0214] 如图4，本发明提供的一种应用上述认证方法的认证系统实施例，包括：

[0215] 读写器401和标签402；

[0216] 读写器包括：

[0217] 第一获取单元4011，用于向标签发送用于获取第一密钥的请求信息；

[0218] 第一接收单元4012，用于接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥；

[0219] 第一解密单元4013，用于对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据；

[0220] 第一判断单元4014，用于判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像；

[0221] 第一生成单元4015，用于生成第二密钥；

[0222] 第二生成单元4016，用于生成密钥因子；

[0223] 第一发送单元4017，用于向标签发送密钥因子；

[0224] 所述标签402包括：

[0225] 第二接收单元4021，用于接收读写器发送的用于获取第一密钥的请求信息；

[0226] 第三生成单元45022，用于对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；

[0227] 第三接收单元4023，用于接收密钥因子；

[0228] 第二解密单元4024，用于对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。

[0229] 本实施例中，认证系统由读写器401和标签402组成，读写器401的第一获取单元4011向标签402发送用于获取第一秘钥的请求信息；标签502的第二接收单元4021接收请求后，第三生成单元4022对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一密钥；读写器401的第一接收单元4012接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一密钥，第一解密单元4013对第一密钥使用第一解密规则进行解密，得到名

片数据及虚拟名片数据，第一判断单元4014判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像，第一生成单元4015生成第二密钥，第二生成单元4016生成密钥因子，第一发送单元4017向标签发送密钥因子；标签402的第三接收单元4023接收密钥因子，第二解密单元4024对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥。读写器401和标签402生成的共享密钥，此方法可用于单个标签、批量标签及群组标签密钥的生成，整个认证系统通过简单的运算，降低了标签成本与计算量。

[0230] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0231] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不处理。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0232] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0233] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0234] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0235] 以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

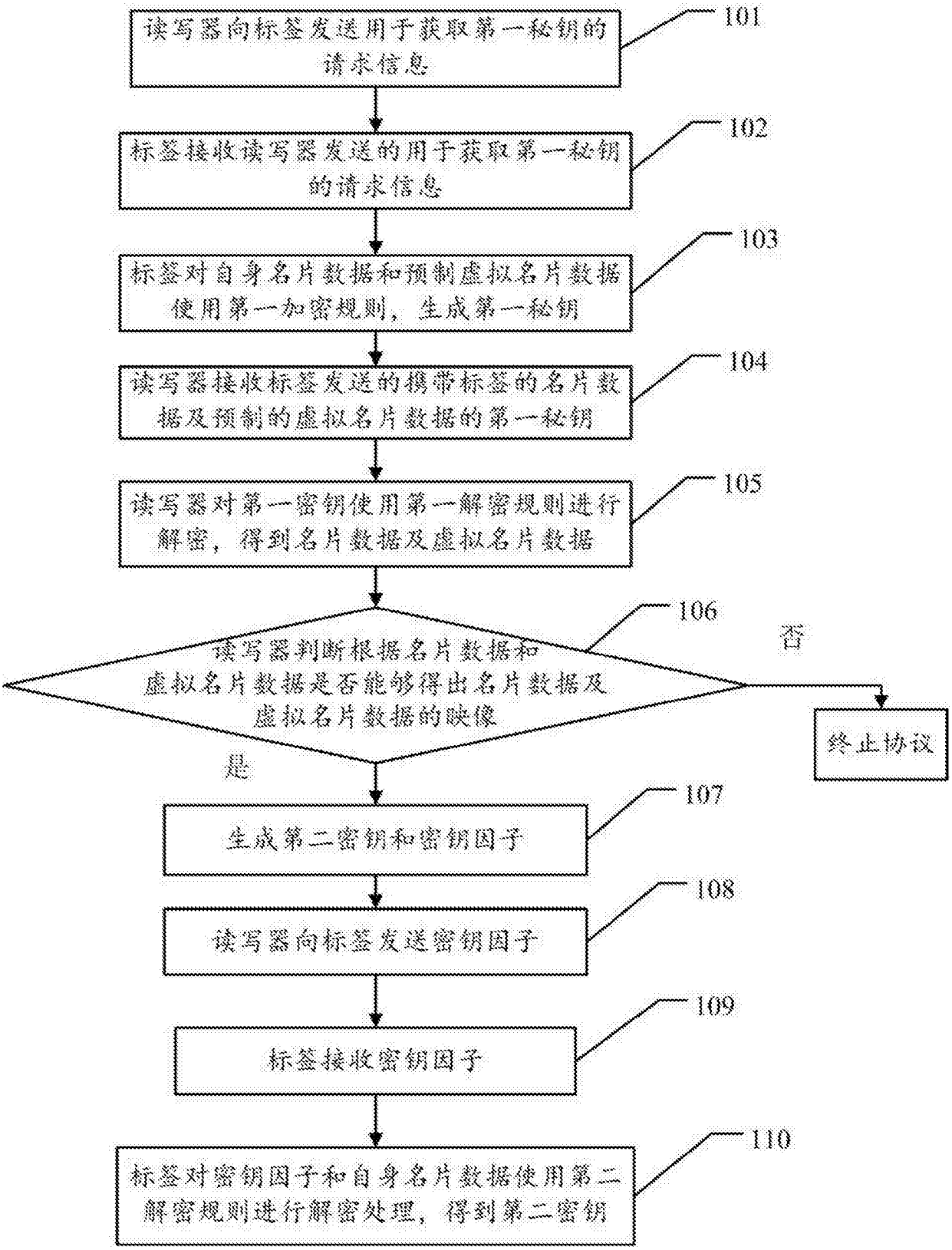

读写器向标签发送用于获取第一秘钥的请求信息
101
标签接收读写器发送的用于获取第一秘钥的请求信息
102
标签对自身名片数据和预制虚拟名片数据使用第一加密规则，生成第一秘钥
103
读写器接收标签发送的携带标签的名片数据及预制的虚拟名片数据的第一秘钥
104
读写器对第一密钥使用第一解密规则进行解密，得到名片数据及虚拟名片数据
105
读写器判断根据名片数据和虚拟名片数据是否能够得出名片数据及虚拟名片数据的映像
106
否
终止协议
是
生成第二密钥和密钥因子
107
读写器向标签发送密钥因子
108
标签接收密钥因子
109
标签对密钥因子和自身名片数据使用第二解密规则进行解密处理，得到第二密钥
110

图1

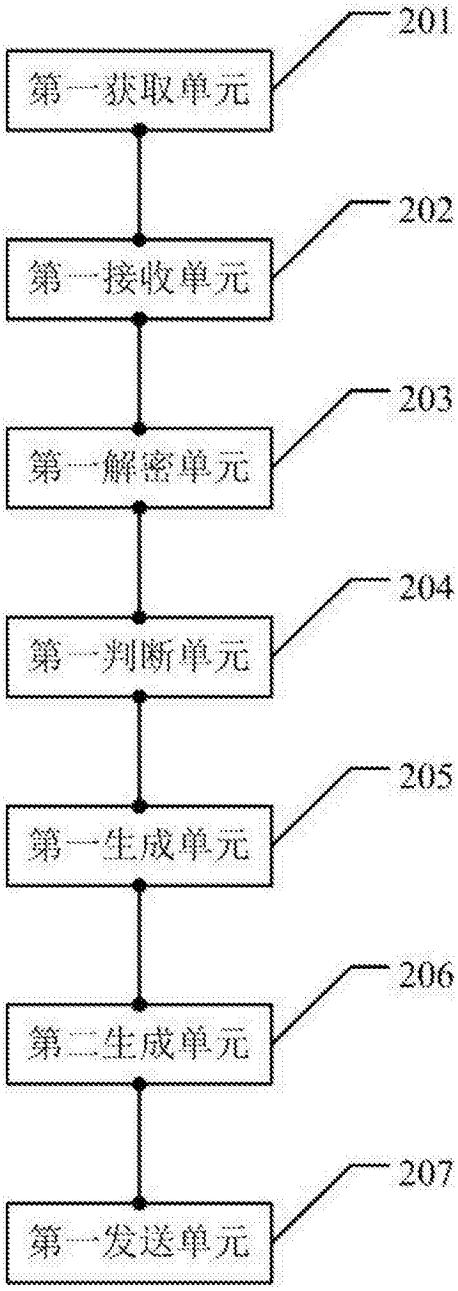

201
第一获取单元
202
第一接收单元
203
第一解密单元
204
第一判断单元
205
第一生成单元
206
第二生成单元
207
第一发送单元

图2

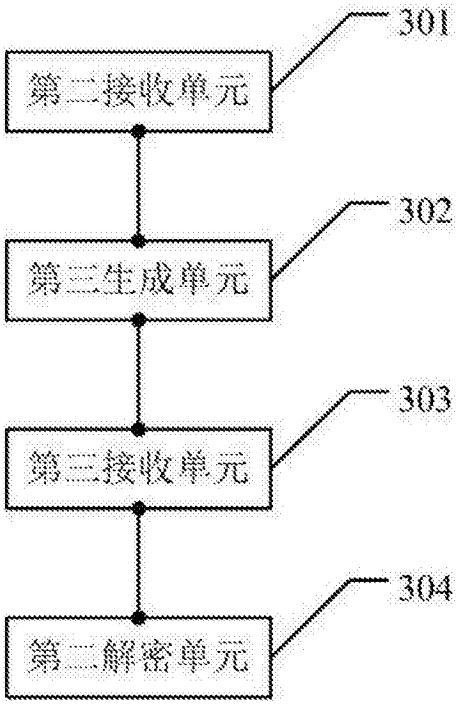

301
第二接收单元
302
第三生成单元
303
第三接收单元
304
第二解密单元

图3

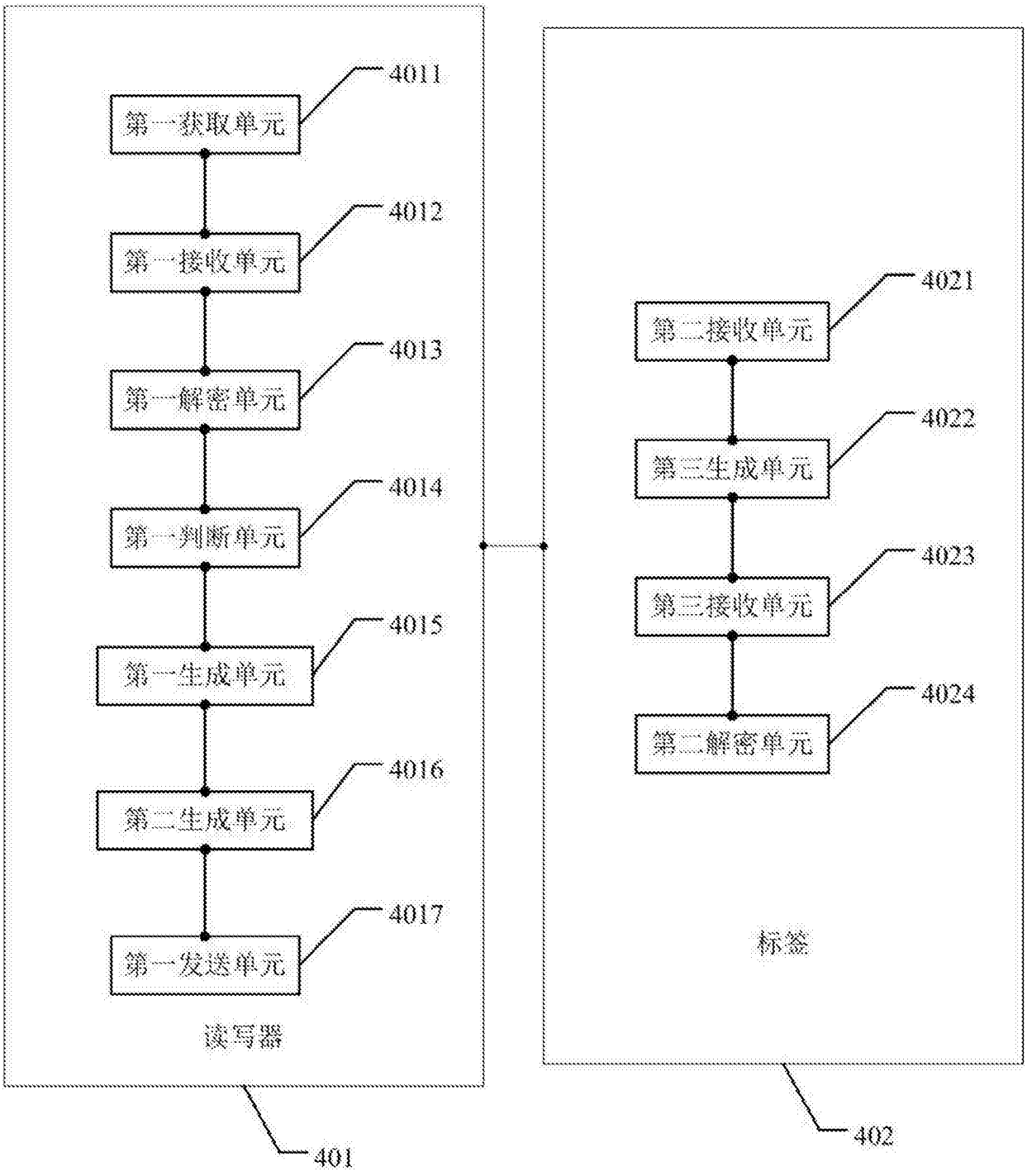

4011
第一获取单元
4012
第一接收单元
4013
第一解密单元
4014
第一判断单元
4015
第一生成单元
4016
第二生成单元
4017
第一发送单元
读写器
401
4021
第二接收单元
4022
第三生成单元
4023
第三接收单元
4024
第二解密单元
标签
402

图4