(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 105404907 B
(45)授权公告日 2018.08.21

(21)申请号 201510705749.0

(22)申请日 2015.10.27

(65)同一申请的已公布的文献号
申请公布号 CN 105404907 A

(43)申请公布日 2016.03.16

(73)专利权人 上海象形通讯科技股份有限公司
地址 201416 上海市奉贤区新寺镇目华路500号C区26室

(72)发明人 聂明

(74)专利代理机构 上海国智知识产权代理事务所(普通合伙) 31274
代理人 潘建玲

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

(56)对比文件
CN 103150655 A,2013.06.12,
CN 102629332 A,2012.08.08,
CN 1728162 A,2006.02.01,
CN 104064031 A,2014.09.24,
CN 204204199 U,2015.03.11,

审查员 尹川

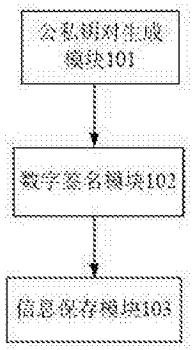
权利要求书2页 说明书5页 附图4页

(54)发明名称

RFID电子车牌生成系统、方法及车牌识别系统、方法

(57)摘要

本发明公开了一种RFID电子车牌生成系统、方法及车牌识别系统、方法，该车牌生成系统包括：公私钥对生成模块，基于RFID芯片的唯一ID号码生成公私钥对；数字签名模块，利用芯片的私钥对车牌的相关信息进行数字签名；信息保存模块，将数字签名后的信息和用户账户信息、车牌信息保存于该RFID芯片或后台服务器，本发明通过将车辆的车牌信息、车主信息和数据签名信息植入电子车牌的RFID芯片中，于读写器读取时，首先对车牌中的RFID芯片内的签名信息进行验证，完成相互的签名验证，并用读写器的公钥对电子车牌信息进行加密传送，签名验证的过程和加密传送保证了读写器与电子标签之间的数据安全，防止数据被窃取和篡改。




CN 105404907 B

1.一种RFID电子车牌生成系统,包括:

公私钥对生成模块,基于RFID芯片的唯一ID号码生成公私钥对;

数字签名模块,利用芯片的私钥对车牌的相关信息进行数字签名;

信息保存模块,将数字签名后的信息和用户账户信息、车牌信息保存于该RFID芯片或后台服务器。

2.如权利要求1所述的RFID电子车牌生成系统,其特征在于:若该RFID芯片存储空间小,则该信息保存模块将该RFID芯片的ID号码及签名信息保存在RFID芯片中,其他信息加密保存在后台服务器。

3.一种RFID电子车牌生成方法,包括如下步骤:

基于RFID芯片的唯一ID号码生成公私钥对;

利用RFID芯片的私钥对车牌的相关信息进行数字签名;

将数字签名后的信息和用户账户信息、车牌信息写入RFID芯片或后台服务器。

4.如权利要求3所述的RFID电子车牌生成方法,其特征在于:若RFID芯片存储空间小,该RFID芯片的ID号码及签名信息保存在该RFID芯片中,其他信息加密保存在后台服务器。

5.一种RFID电子车牌识别系统,包括:

RFID电子车牌,具有唯一ID 号码,其基于该ID号码生成公私钥对,利用芯片的私钥对车牌的相关信息进行数字签名,并将签名后的信息和用户账户信息、车牌信息写入RFID芯片或后台服务器形成;

读写器,用于读取该RFID电子车牌,对将读取的车牌信息进行验证,采用RFID芯片的ID号码和公钥矩阵运算出公钥,利用公钥对签名信息进行验证。

6.如权利要求5所述的一种RFID电子车牌识别系统,其特征在于:该系统还包括云平台,该读写器于验证成功后,将读取到的车牌信息传至该云平台,该云平台可根据用户账户信息找到对应的关联用户。

7.如权利要求6所述的一种RFID电子车牌识别系统,其特征在于:当该读写器验证失败时,发出警告提示。

8.一种RFID电子车牌识别方法,包括如下步骤:

步骤一,当RFID电子车牌进入读写器的读写区域内时,电子车牌感应后发起随机序列和电子车牌的ID号码,并用自己的私钥进行签名,读写器通过收到随机签名和ID号码,用读写器内部的公钥矩阵结合该ID号码算出该电子车牌的公钥,进行验签;

步骤二,验签通过后,读写器将自己的ID号码,电子车牌发送的随机序列和读写器自己的私钥的签名发给该RFID电子车牌,电子车牌收到自己发送的随机序列,以及读写器的ID号码,结合公钥矩阵算出读写器的公钥,进行验签;

步骤三,验签通过后,RFID电子车牌用读写器的公钥对RFID车牌芯片内的车辆信息进行加密,传给读写器;读写器读取该RFID电子车牌的车牌信息,用自己的私钥进行解密,用RFID车牌的公钥进行验签。

9.如权利要求8所述的RFID电子车牌识别方法,其特征在于:于步骤三之后,还包括如下步骤:若验证成功,读写器将读取到的车牌数据加密后传送至云平台,由云平台对数据解密后根据账户信息找到对应的关联用户。

10.如权利要求8所述的RFID电子车牌识别方法,其特征在于:上述每个步骤中,若验证

失败，则流程结束，并发出警告提示。

# RFID电子车牌生成系统、方法及车牌识别系统、方法

## 技术领域

[0001] 本发明关于一种RFID电子车牌生成系统、方法及车牌识别系统、方法，特别是涉及一种基于标识的非对称加密的RFID电子车牌生成系统、方法及车牌识别系统、方法。

## 背景技术

[0002] 随着经济的飞速发展，汽车的持有量在中国呈现着急剧增长的趋势，2003年汽车保有量达到1219万辆，2010年，我国汽车的保有量达到了7000万辆，截至2014年底，全国机动车保有量达2.64亿辆。

[0003] 目前我国的车辆管理都采用车牌号管理，新车购买时注册登记，取得车辆牌照后可正常上路使用，车辆持有者信息、驾驶证和所持车牌号码在相关单位中备案。在车辆的日常使用中，涉及到车检、缴费、交通违章等情况时，车主需要递交相关资料给相关机构，相关机构和单位则通过车主及车辆资料得到想要的信息，对该车辆进行处理。

[0004] 这种做法存在一定的弊端和不足，一、车辆的驾驶证、行驶证等证件，在使用过程中容易磨损造成字体不清或者信息辨认不出，更有甚者出现证件丢失的状况，需要紧急使用证件时使用者无法提供出正确信息，给使用者带来极大困扰，必要情况下还需要车主集齐证件资料去车辆管理中心换取新的证件；二、以现有的状态下，交通执法系统没有实现全国各地车辆管理相互连通，车主信息与车牌号码没有实时绑定，车牌号容易被伪造，出现套牌车、冒牌车、隐形车辆，当发生交通意外时，交通执法者无法在第一时间了解车辆具体信息，对执法效率和速度产生一定的影响；

[0005] 近年来由于智慧交通与智慧城市的热门普及，智能设备也渐渐的出现在车辆相关系统中。交通系统将RFID射频识别技术应用于车牌识别，但是在实际实施过程中，具有极大隐患，采集车辆信息较为混乱，信息采集不够准确，影响系统的正确判断。同时，电子标签与读写器间没有任何认证过程，使得未经授权的读写器可以模仿合法读写器去读取标签内容，在可写标签上甚至可能篡改数据；同样的，读写器也无法鉴别电子标签的合法性，攻击者通过无用的或者错误的标签信息作为响应来欺骗读写器，造成数据的泄露，这些对交通管理会带来严重后果。

## 发明内容

[0006] 为克服上述现有技术存在的不足，本发明之目的在于提供一种RFID电子车牌生成系统、方法及车牌识别系统、方法，其通过将车辆的车牌信息、车主信息和数据签名信息植入RFID芯片中，而RFID芯片在车牌生成的时候贴入车牌中，读写器读取时，首先对车牌中的RFID标签内的签名信息进行验证，签名验证的过程保证了读写器与电子标签之间的数据安全，防止数据被窃取和篡改。

[0007] 为达上述及其它目的，本发明提出一种RFID电子车牌生成系统，包括：

[0008] 公私钥对生成模块，基于RFID芯片的唯一ID号码生成公私钥对；

[0009] 数字签名模块，利用芯片的私钥对车牌的相关信息进行数字签名；

[0010] 信息保存模块，将数字签名后的信息和用户账户信息、车牌信息保存于该RFID芯片或后台服务器。

[0011] 进一步地，若该RFID芯片存储空间小，则该信息保存模块将该RFID芯片的ID号码及签名信息保存在RFID芯片中，其他信息加密保存在后台服务器。

[0012] 为达到上述目的，本发明还提供一种RFID电子车牌生成方法，包括如下步骤：

[0013] 基于RFID芯片的唯一ID号码生成公私钥对；

[0014] 利用RFID芯片的私钥对车牌的相关信息进行数字签名；

[0015] 将数字签名后的信息和用户账户信息、车牌信息写入RFID芯片或后台服务器。

[0016] 进一步地，若RFID芯片存储空间小，该RFID芯片的ID号码及签名信息保存在该RFID芯片中，其他信息加密保存在后台服务器。

[0017] 为达到上述目的，本发明还提供一种RFID电子车牌识别系统，包括：

[0018] RFID电子车牌，具有唯一ID 号码，其基于该ID号码生成公私钥对，利用芯片的私钥对车牌的相关信息进行数字签名，并将签名后的信息和用户账户信息、车牌信息写入RFID芯片或后台服务器形成；

[0019] 读写器，用于读取该RFID电子车牌，对将读取的车牌信息进行验证，采用RFID芯片的ID号码和公钥矩阵运算出公钥，利用公钥对签名信息进行验证。

[0020] 进一步地，该系统还包括云平台，该读写器于验证成功后，将读取到的车牌信息传至该云平台，该云平台可根据用户账户信息找到对应的关联用户。

[0021] 进一步地，当该读写器验证失败时，发出警告提示。

[0022] 为达到上述目的，本发明还提供一种RFID电子车牌识别方法，包括如下步骤：

[0023] 步骤一，当RFID电子车牌进入读写器的读写区域内时，电子车牌感应后发起随机序列和电子车牌的ID号码，并用自己的私钥进行签名，读写器通过收到随机签名和ID号码，用读写器内部的公钥矩阵结合该ID号码算出该电子车牌的公钥，进行验签；

[0024] 步骤二，验签通过后，读写器将自己的ID号码，电子车牌发送的随机序列和读写器自己的私钥的签名发给该RFID电子车牌，电子车牌收到自己发送的随机序列，以及读写器的ID号码，结合公钥矩阵算出读写器的公钥，进行验签；

[0025] 步骤三，验签通过后，RFID电子车牌用读写器的公钥对RFID车牌芯片内的车辆信息进行加密，传给读写器；读写器读取该RFID电子车牌的车牌信息，用读写器自己的私钥进行解密，用RFID车牌的公钥进行验签；

[0026] 进一步地，于步骤三之后，还包括如下步骤：若验证成功，读写器将读取到的车牌数据加密后传送至云平台，由云平台解密数据后，根据账户信息找到对应的关联用户。

[0027] 进一步地，上述每个步骤中：若验证失败，则流程结束，并发出警告提示。

[0028] 与现有技术相比，本发明一种RFID电子车牌生成系统、方法及车牌识别系统、方法，其通过将车辆的车牌信息、车主信息和数据签名信息植入RFID芯片中，而RFID芯片在车牌生成的时候贴入车牌中，读写器读取时，首先对车牌中的RFID标签内的签名信息进行验证，签名验证的过程保证了读写器与电子标签之间的数据安全，防止数据被窃取和篡改。

## 附图说明

[0029] 图1为本发明一种RFID电子车牌生成系统的架构示意图；

[0030] 图2为本发明一种RFID电子车牌生成方法的步骤流程图；

[0031] 图3为本发明一种RFID电子车牌识别系统的系统架构图；

[0032] 图4为本发明一种RFID电子车牌识别方法的步骤流程图；

[0033] 图5为本发明第一具体实施例中RFID电子车牌在加油站的应用流程图；

[0034] 图6为本发明第二具体实施例中RFID电子车牌在停车场的应用流程图。

## 具体实施方式

[0035] 以下通过特定的具体实例并结合附图说明本发明的实施方式，本领域技术人员可由本说明书所揭示的内容轻易地了解本发明的其它优点与功效。本发明亦可通过其它不同的具体实例加以施行或应用，本说明书中的各项细节亦可基于不同观点与应用，在不背离本发明的精神下进行各种修饰与变更。

[0036] 图1为本发明一种RFID电子车牌生成系统的架构示意图。如图1所示，本发明一种RFID电子车牌生成系统，包括：公私钥对生成模块101、数字签名模块102以及信息保存模块103。

[0037] 其中，公私钥对生成模块101，基于RFID芯片的唯一ID号码生成公私钥对；数字签名模块102利用芯片的私钥对车牌的相关信息进行数字签名；信息保存模块103将数字签名后的信息和用户账户信息、车牌信息写入RFID芯片，该 RFID芯片可贴于车牌上形成RFID电子车牌。在此需说明的是，如果RFID芯片存储空间小，则信息保存模块103将该RFID的ID号码及签名信息保存在RFID芯片中， 其他信息加密保存在后台服务器。

[0038] 图2为本发明一种RFID电子车牌生成方法的步骤流程图。如图2所示，本发明一种RFID电子车牌生成方法，包括如下步骤：

[0039] 步骤201，基于RFID芯片的唯一ID号码生成公私钥对；

[0040] 步骤202，利用RFID芯片的私钥对车牌的相关信息进行数字签名；

[0041] 步骤203，将数字签名后的信息和用户账户信息、车牌信息写入RFID芯片，当然，如果RFID芯片存储空间小，可将该RFID的ID号码及签名信息保存在RFID芯片中， 其他信息加密保存在后台服务器。

[0042] 图3为本发明一种RFID电子车牌识别系统的系统架构图。如图3所示，本发明一种RFID电子车牌识别系统，包括：RFID电子车牌30以及读写器31。

[0043] 其中，RFID电子车牌30具有唯一ID 号码，其基于该ID号码生成公私钥对，利用芯片的私钥对车牌的相关信息进行数字签名，并将签名后的信息和用户账户信息、车牌信息等写入RFID芯片中形成；读写器31用于读取RFID电子车牌30，其将读取的车牌信息进行验证，即用RFID芯片的ID号码和公钥矩阵运算出公钥，利用公钥对签名信息进行验证。

[0044] 较佳的，本发明之RFID电子车牌识别系统还包括云平台32，读写器31于验证成功后，将读取到的车牌信息传至云平台31，云平台31则可根据用户账户信息找到对应的关联用户。

[0045] 图4为本发明一种RFID电子车牌识别方法的步骤流程图。如图4所示，本发明一种RFID电子车牌识别方法，包括如下步骤：

[0046] 步骤401，当RFID电子车牌进入读写器的读写区域内时，电子车牌感应后发起随机序列和电子车牌的ID号码，并用自己的私钥进行签名，读写器通过收到随机签名和ID号码，

用读写器内部的公钥矩阵结合该ID号码算出该电子车牌的公钥，进行验签；

[0047] 步骤402，验签通过后，读写器将自己的ID号码，电子车牌发送的随机序列和读写器自己的私钥的签名发给该RFID电子车牌，电子车牌收到自己发送的随机序列，以及读写器的ID号码，结合公钥矩阵算出读写器的公钥，进行验签；

[0048] 步骤403，

[0049] 验签通过后，RFID电子车牌用读写器的公钥对RFID车牌芯片内的车辆信息进行加密，传给读写器；读写器读取该RFID电子车牌的车牌信息，用读写器自己的私钥进行解密，用RFID车牌的公钥进行验签；读写取读取该RFID电子车牌的车牌信息.若验证成功，读写器将读取到的车牌数据传送至云平台，由云平台根据账户信息找到对应的关联用户；若验证失败，则流程结束，并发出警告提示。

[0050] 图5为本发明第一具体实施例中RFID电子车牌在加油站的应用流程图：

[0051] 1、张三新买了一辆车，车辆管理中心给张三的新车进行登记与车牌发放，车牌的内容如下：根据RFID的ID得出私钥，用私钥对车辆相关信息进行签名，将签名信息与用户在云平台的账户信息、车牌信息一起写入RFID芯片中，此RFID芯片贴于车牌上，如果芯片存储空间小，则只需要保存该RFID的ID号以及签名，其他信息加密保存在后台服务器。

[0052] 2、当张三开车去加油站加油，将车辆停在加油设备旁边。加油设备旁边有RFID读头(读写器)，对车牌自动读取。

[0053] 3、读头将读取的车牌信息进行验证，即用RFID的ID和公钥矩阵运算出公钥，用公钥对签名信息进行验证。若验证失败，则流程结束，并发出警告提示；

[0054] 4、若验证成功，读头将读取到的车辆数据传至云平台，云平台根据账户信息找到对应的关联用户，即找到张三在云平台中的信息；

[0055] 5、加油设备将加油金额传至云平台，云平台向该张三发送扣款请求；

[0056] 6、此时张三可通过多种方式付款：手机APP或者刷银行卡等，完成付款动作；

[0057] 7、付款成功，云平台扣款成功，告知加油设备，流程结束。

[0058] 图6为本发明第二具体实施例中RFID电子车牌在停车场的应用流程图：

[0059] 1、张三开车进入停车场，停车场入口的RFID读头设备(读写器)读取电子车牌内容；

[0060] 2、读头对电子车牌信息进行验证：用RFID的ID与公钥矩阵进行运算，得到该RFID的公钥，对电子车牌的签名信息进行验证；

[0061] 3、若验证失败，人工进行干预，流程结束；若验证成功，停车场的道闸放行，读头将电子车牌信息及停车开始时间传至云平台；

[0062] 4、云平台根据账户信息找到对应的用户信息，即找到张三在云平台中的信息；

[0063] 5、张三开车驶出停车场时，停车场出口处的RFID读头再次读取电子车牌信息，进行再次验证，用RFID的ID和公钥矩阵运算出公钥，用公钥对签名信息进行验证；

[0064] 6、若验证失败，则人工干预，流程结束；若验证通过，读头将电子车牌信息及停车结束时间传至云平台；

[0065] 7、云平台根据账户信息找到张三的停车信息，根据停车时间进行计算，得出停车金额，并向张三发送扣款请求；

[0066] 8、张三可使用手机app或者刷银行卡付款；

[0067] 9、付款成功后，云平台向读头设备发送扣款成功的通知，停车场的道闸放行，车子驶出，流程结束。

[0068] 与现有技术相比，本发明具有如下有益效果：

[0069] 1、每个RFID芯片有唯一ID号码，基于ID生成公私钥对，私钥进行数字签名，公钥用来验证，保证了读头和RFID芯片通信过程中信息的合法性；

[0070] 2、电子车牌中包含车主的信息、车辆的信息和驾驶员的信息，实现了人、证、车的绑定，防止了车辆盗用，防止出现套牌车、冒牌车、盗牌车等，在车辆安全管理方面起到很大的作用；

[0071] 3、防拆卸：每个RFID芯片都不可二次使用，一旦毁坏就不能再正常工作，避免反复使用或者另作它用，确保每个芯片对应一部车辆；

[0072] 4、电子车牌包含的车辆及车主的全部信息，可用读头即时认证读出，在停车场、加油站、交通道路、高速收费等处能方便、迅速的获得该车的全部信息，一来便于判断车辆的合法性，便于车辆异地管理，给交通执法带来极大便利；二来提高公共场所相关机构办事效率，极大的降低了管理的成本，为车辆规范化、智能化管理做出巨大贡献。

[0073] 上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何本领域技术人员均可在不违背本发明的精神及范畴下，对上述实施例进行修饰与改变。因此，本发明的权利保护范围，应如权利要求书所列。

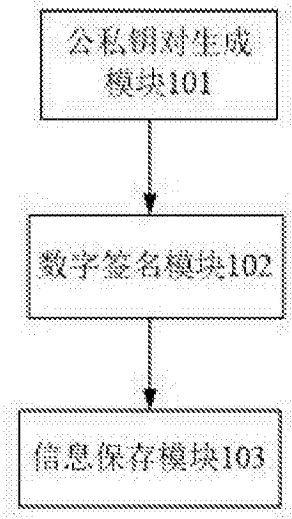

公私钥对生成模块101
数字签名模块102
信息保存模块103

图1

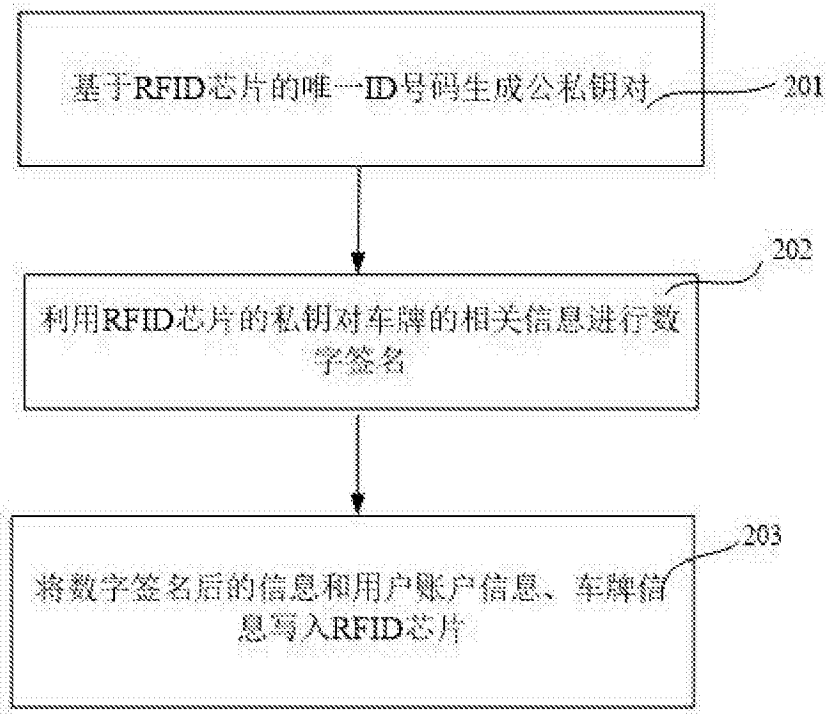

基于RFID芯片的唯一ID号码生成公私钥对
201
利用RFID芯片的私钥对车牌的相关信息进行数字签名
202
将数字签名后的信息和用户账户信息、车牌信息写入RFID芯片
203

图2

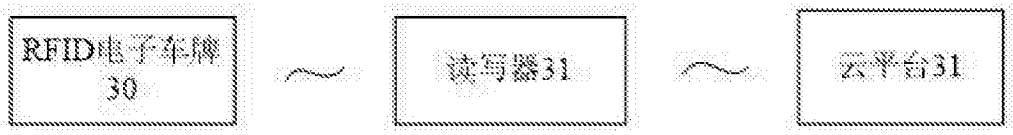

RFID电子车牌30
读写器31
云平台31

图3

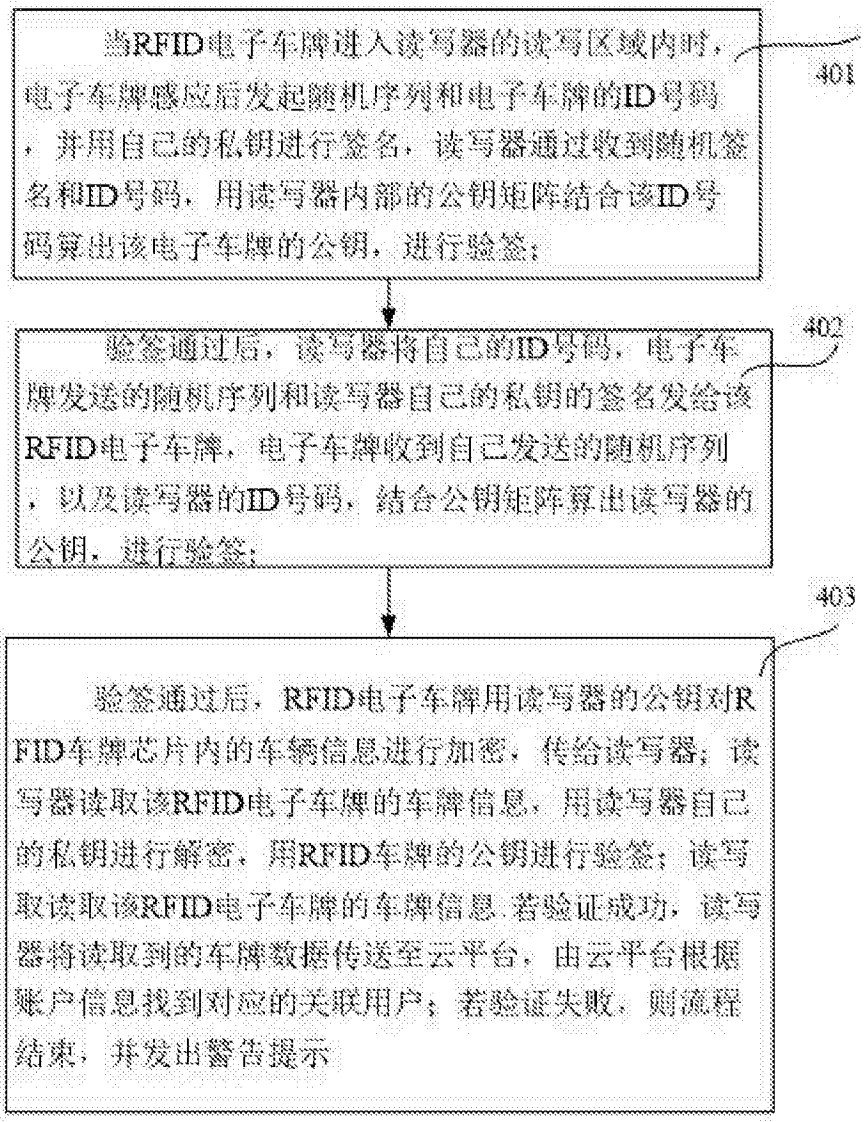

当RFID电子车牌进入读写器的读写区域内时，电子车牌感应后发起随机序列和电子车牌的ID号码，并用自己的私钥进行签名，读写器通过收到随机签名和ID号码，用读写器内部的公钥矩阵结合该ID号码算出该电子车牌的公钥，进行验签；
401
验签通过后，读写器将自己的ID号码，电子车牌发送的随机序列和读写器自己的私钥的签名发给该RFID电子车牌，电子车牌收到自己发送的随机序列，以及读写器的ID号码，结合公钥矩阵算出读写器的公钥，进行验签；
402
验签通过后，RFID电子车牌用读写器的公钥对RFID车牌芯片内的车辆信息进行加密，传给读写器；读写器读取该RFID电子车牌的车牌信息，用读写器自己的私钥进行解密，用RFID车牌的公钥进行验签；读写取读取该RFID电子车牌的车牌信息 若验证成功，读写器将读取到的车牌数据传送至云平台，由云平台根据账户信息找到对应的关联用户；若验证失败，则流程结束，并发出警告提示
403

图4

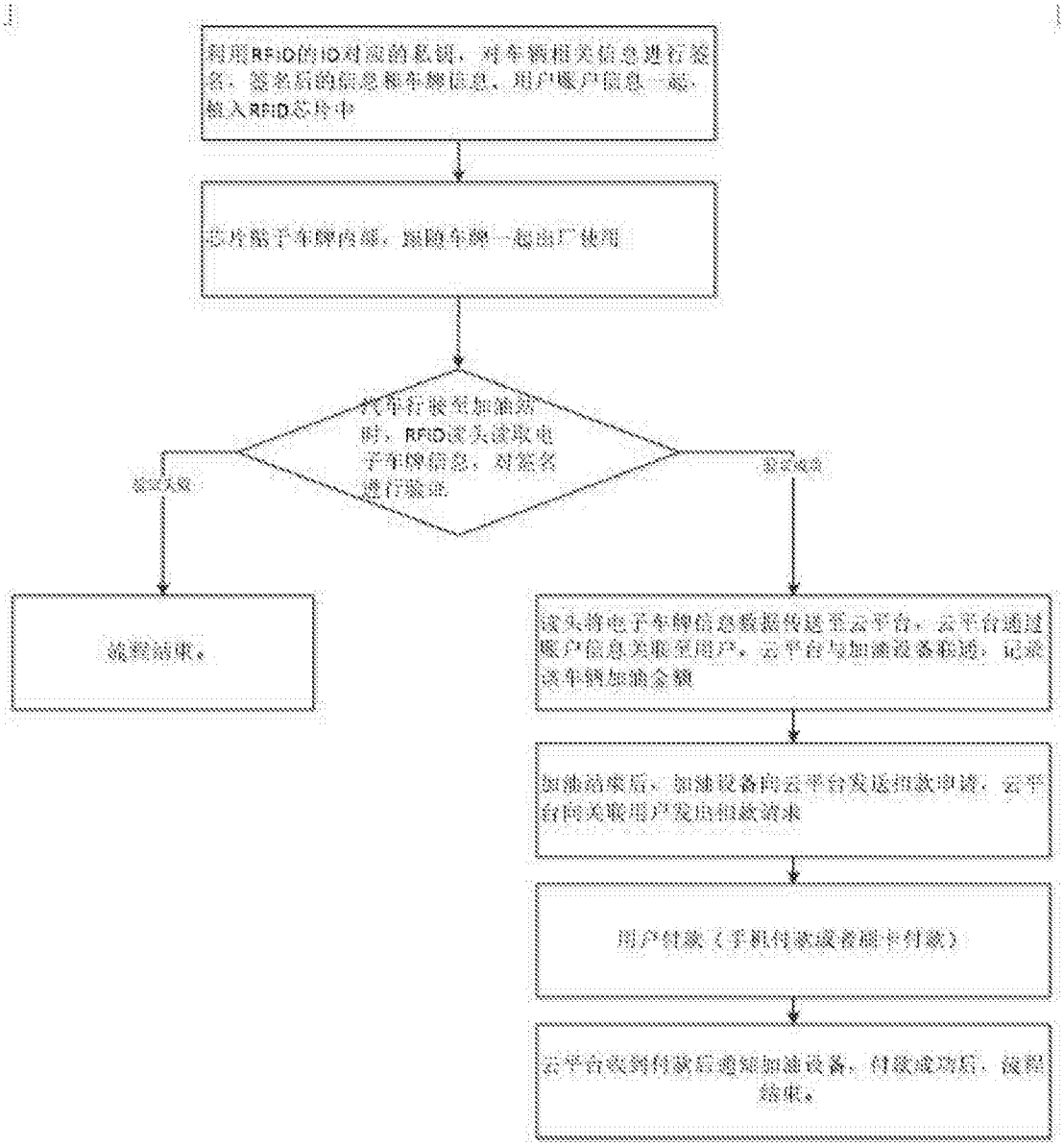

利用RFID的ID对应的机制，对车辆相关信息进行签名，签名后的信息和车牌信息、用户账户信息一起，写入RFID芯片中
芯片贴于车牌内部，随随车牌一起出厂使用
汽车行驶至加油站时，RFID读头读取电子车牌信息，对签名进行验证
验证失败
验证成功
流程结束。
读头将电子车牌信息数据传送至云平台，云平台通过账户信息关联至用户，云平台与加油设备联通，记录该车辆加油金额
加油结束后，加油设备向云平台发送扣款申请，云平台向关联用户发出扣款请求
用户付款（手机付款或者银卡付款）
云平台收到付款后通知加油设备，付款成功后，流程结束。

图5

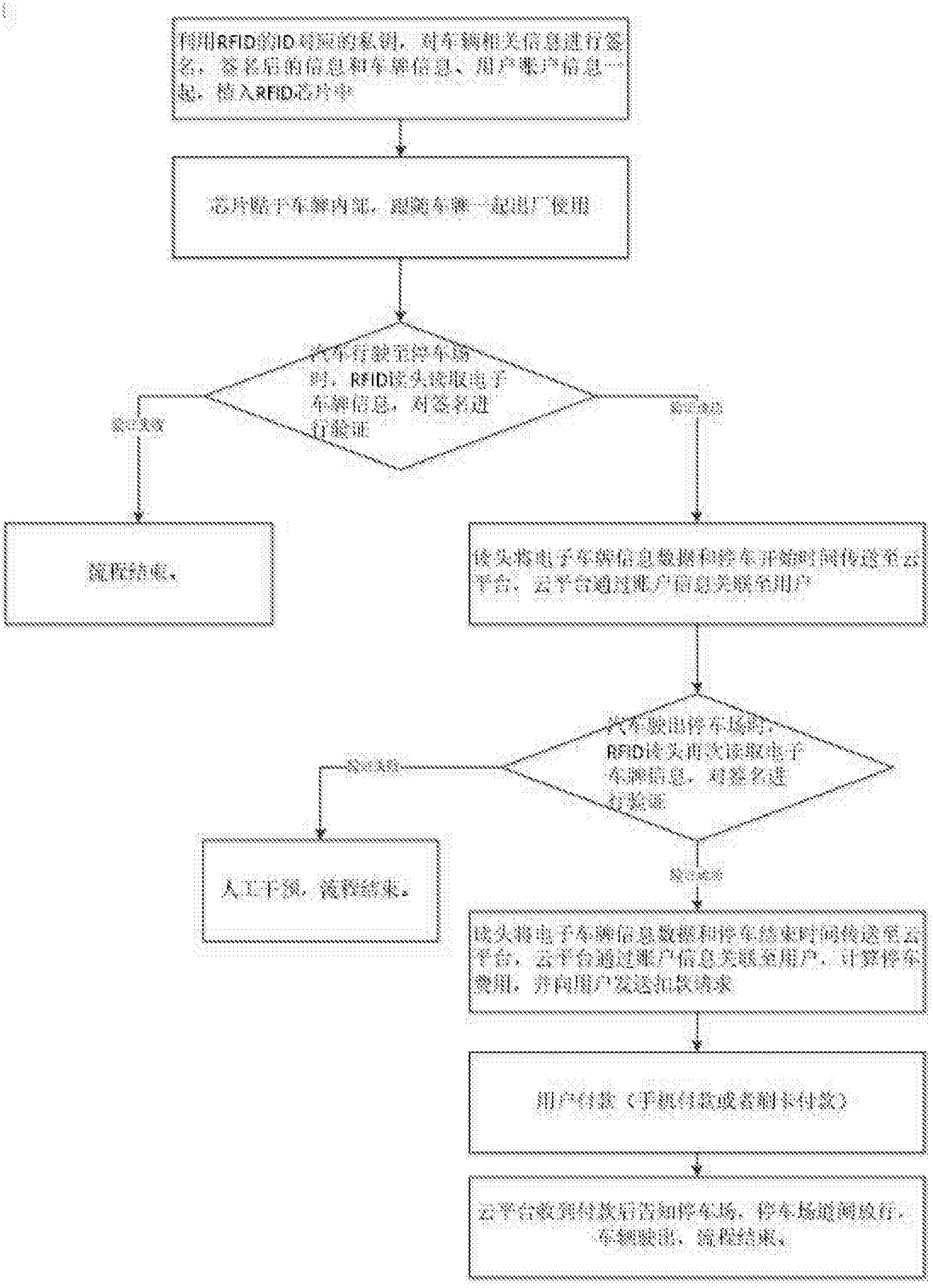

利用RFID的ID对应的私钥，对车辆相关信息进行签名，签名后的信息和车辆信息、用户账户信息一起，烧入RFID芯片中
芯片贴于车辆内壁，随车辆一起出厂使用
汽车行驶至停车场时，RFID读头读取电子车牌信息，对签名进行验证
验证失败
验证成功
流程结束。
读头将电子车牌信息数据和停车开始时间传送至云平台，云平台通过账户信息关联至用户
汽车驶出停车场时，RFID读头再次读取电子车牌信息，对签名进行验证
验证失败
人工干预，流程结束。
验证成功
读头将电子车牌信息数据和停车结束时间传送至云平台，云平台通过账户信息关联至用户，计算停车费用，并向用户发送扣款请求
用户付款（手机付款或者刷卡付款）
云平台收到付款后告知停车场，停车场道闸放行，车辆驶出，流程结束。

图6