(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115376226 A
(43)申请公布日 2022.11.22

(21)申请号 202211012816.7

(22)申请日 2022.08.23

(71)申请人 芜湖雄狮汽车科技有限公司
地址 241009 安徽省芜湖市经济技术开发区鞍山南路
申请人 奇瑞汽车股份有限公司

(72)发明人 陈万东 陈德石 李拓

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 于腾昊

(51)Int.Cl.
G07C 9/00(2020.01)
H04W 4/48(2018.01)
H04W 4/80(2018.01)
H04W 12/06(2021.01)

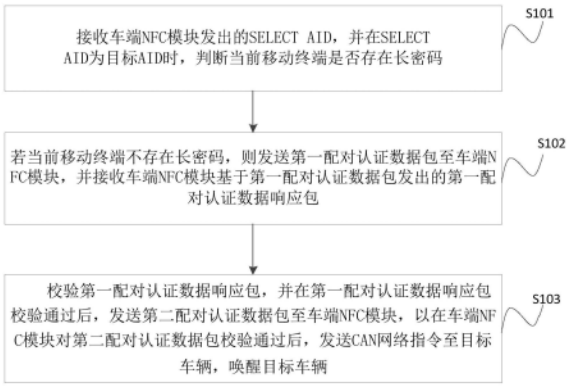
权利要求书2页 说明书8页 附图3页

(54)发明名称

NFC车钥匙认证方法、装置、车辆及存储介质

(57)摘要

本申请涉及一种NFC车钥匙认证方法、装置、车辆及存储介质，包括：接收车端NFC模块发出的SELECT AID，SELECT AID为目标AID时，判断当前移动终端是否存在长密码；若当前移动终端不存在长密码，发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块基于第一配对认证数据包发出的第一配对认证数据响应包；校验第一配对认证数据响应包，第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。



CN 115376226 A

1.一种NFC车钥匙认证方法,其特征在于,包括以下步骤:

接收车端NFC模块发出的SELECT AID,并在所述SELECT AID为目标AID时,判断当前移动终端是否存在长密码;

若所述当前移动终端不存在所述长密码,则发送第一配对认证数据包至所述车端NFC模块,并接收所述车端NFC模块基于所述第一配对认证数据包发出的第一配对认证数据响应包;

校验所述第一配对认证数据响应包,并在所述第一配对认证数据响应包校验通过后,发送第二配对认证数据包至所述车端NFC模块,以在所述车端NFC模块对所述第二配对认证数据包校验通过后,发送CAN网络指令至目标车辆,唤醒所述目标车辆。

2.根据权利要求1所述的方法,其特征在于,在所述车端NFC模块对所述第二配对认证数据包校验通过后,还包括:

接收所述车端NFC模块发送的基于所述第二配对认证数据包生成的第二配对认证数据响应包;

校验所述第二配对认证数据响应包,并在所述第二配对认证数据响应包检验通过后,从所述第二配对认证数据响应包获取目标长密码,并将所述目标长密码存储在所述当前移动终端。

3.根据权利要求1所述的方法,其特征在于,还包括:

若所述当前移动终端存在所述长密码,则构造11数据包,并发送所述11数据包至所述车端NFC模块;

接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包;

校验所述11数据响应包,并在所述11数据响应包检验通过后,从所述11数据响应包中获取所述目标长密码,并将所述目标长密码存储在当前移动终端。

4.根据权利要求3所述的方法,其特征在于,在接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包之后,还包括:

发送所述CAN网络指令至所述目标车辆,以唤醒所述目标车辆。

5.根据权利要求3所述的方法,其特征在于,在发送所述11数据包至所述车端NFC模块之后,还包括:

接收所述车端NFC模块校验所述11数据包失败后发送的11数据失败包;

从所述1数据失败包中获取失败原因,并根据所述失败原因构造所述第一配对认证数据包。

6.一种NFC车钥匙认证装置,其特征在于,包括:

判断模块,用于接收车端NFC模块发出的SELECT AID,并在所述SELECT AID为目标AID时,判断当前移动终端是否存在长密码;

第一接收模块,用于若所述当前移动终端不存在所述长密码,则发送第一配对认证数据包至所述车端NFC模块,并接收所述车端NFC模块基于所述第一配对认证数据包发出的第一配对认证数据响应包;

第一发送模块,用于校验所述第一配对认证数据响应包,并在所述第一配对认证数据响应包校验通过后,发送第二配对认证数据包至所述车端NFC模块,以在所述车端NFC模块对所述第二配对认证数据包校验通过后,发送CAN网络指令至目标车辆,唤醒所述目标车

辆。

7.根据权利要求6所述的装置,其特征在于,在所述车端NFC模块对所述第二配对认证数据包校验通过后,所述第一发送模块,具体用于:

接收所述车端NFC模块发送的基于所述第二配对认证数据包生成的第二配对认证数据响应包;

校验所述第二配对认证数据响应包,并在所述第二配对认证数据响应包检验通过后,从所述第二配对认证数据响应包获取目标长密码,并将所述目标长密码存储在所述当前移动终端。

8.根据权利要求6所述的装置,其特征在于,还包括:

第二发送模块,用于若所述当前移动终端存在所述长密码,则构造11数据包,并发送所述11数据包至所述车端NFC模块;

第二接收模块,用于接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包;

存储模块,用于校验所述11数据响应包,并在所述11数据响应包检验通过后,从所述11数据响应包中获取所述目标长密码,并将所述目标长密码存储在当前移动终端。

9.一种车辆,其特征在于,包括存储器、处理器;

其中,所述处理器通过读取所述存储器中存储的可执行程序代码来运行与所述可执行程序代码对应的程序,以用于实现如权利要求1-5中任一所述的NFC车钥匙认证方法。

10.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-5中任一所述的NFC车钥匙认证方法。

NFC车钥匙认证方法、装置、车辆及存储介质

技术领域

[0001] 本申请涉及无钥匙启动系统技术领域，特别涉及一种NFC(Near Field Communication，近场通信)车钥匙认证方法、装置、车辆及存储介质。

背景技术

[0002] 车辆NFC数字钥匙是一种基于NFC近场通信技术，用户使用手机NFC功能或NFC卡片对车辆进行控制。车辆NFC数字钥匙一般包括使用手机NFC或NFC卡片对车辆进行锁车和解锁，对车辆进行一键启动控制等主要功能。

[0003] 然而，由于利用NFC卡以及携带NFC协议的手机都可以作为NFC车钥匙的一个终端，不利于保证财产的安全性，亟待解决。

发明内容

[0004] 本申请提供一种NFC车钥匙认证方法、装置、车辆及存储介质，解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。

[0005] 本申请第一方面实施例提供一种NFC车钥匙认证方法，包括以下步骤：接收车端NFC模块发出的SELECT AID(标准选择指令)，并在所述SELECT AID为目标AID时，判断当前移动终端是否存在长密码；若所述当前移动终端不存在所述长密码，则发送第一配对认证数据包至所述车端NFC模块，并接收所述车端NFC模块基于所述第一配对认证数据包发出的第一配对认证数据响应包；校验所述第一配对认证数据响应包，并在所述第一配对认证数据响应包校验通过后，发送第二配对认证数据包至所述车端NFC模块，以在所述车端NFC模块对所述第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒所述目标车辆。

[0006] 可选地，在所述车端NFC模块对所述第二配对认证数据包校验通过后，还包括：接收所述车端NFC模块发送的基于所述第二配对认证数据包生成的第二配对认证数据响应包；校验所述第二配对认证数据响应包，并在所述第二配对认证数据响应包检验通过后，从所述第二配对认证数据响应包获取目标长密码，并将所述目标长密码存储在所述当前移动终端。

[0007] 可选地，上述的NFC车钥匙认证方法，还包括：若所述当前移动终端存在所述长密码，则构造11数据包，并发送所述11数据包至所述车端NFC模块；接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包；校验所述11数据响应包，并在所述11数据响应包检验通过后，从所述11数据响应包中获取所述目标长密码，并将所述目标长密码存储在当前移动终端。

[0008] 可选地，在接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包之后，还包括：发送所述CAN网络指令至所述目标车辆，以唤醒所述目标车辆。

[0009] 可选地，在发送所述11数据包至所述车端NFC模块之后，还包括：接收所述车端NFC模块校验所述11数据包失败后发送的11数据失败包；从所述1数据失败包中获取失败原因，

并根据所述失败原因构造所述第一配对认证数据包。

[0010] 本申请第二方面实施例提供一种NFC车钥匙认证装置，包括：判断模块，用于接收车端NFC模块发出的SELECT AID，并在所述SELECT AID为目标AID时，判断当前移动终端是否存在长密码；第一接收模块，用于若所述当前移动终端不存在所述长密码，则发送第一配对认证数据包至所述车端NFC模块，并接收所述车端NFC模块基于所述第一配对认证数据包发出的第一配对认证数据响应包；第一发送模块，用于校验所述第一配对认证数据响应包，并在所述第一配对认证数据响应包校验通过后，发送第二配对认证数据包至所述车端NFC模块，以在所述车端NFC模块对所述第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒所述目标车辆。

[0011] 可选地，在所述车端NFC模块对所述第二配对认证数据包校验通过后，所述第一发送模块，具体用于：接收所述车端NFC模块发送的基于所述第二配对认证数据包生成的第二配对认证数据响应包；校验所述第二配对认证数据响应包，并在所述第二配对认证数据响应包检验通过后，从所述第二配对认证数据响应包获取目标长密码，并将所述目标长密码存储在所述当前移动终端。

[0012] 可选地，上述的NFC车钥匙认证装置，还包括：第二发送模块，用于若所述当前移动终端存在所述长密码，则构造11数据包，并发送所述11数据包至所述车端NFC模块；第二接收模块，用于接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包；存储模块，用于校验所述11数据响应包，并在所述11数据响应包检验通过后，从所述11数据响应包中获取所述目标长密码，并将所述目标长密码存储在当前移动终端。

[0013] 可选地，在接收所述车端NFC模块校验所述11数据包通过后发送的11数据响应包之后，还包括：发送所述CAN网络指令至所述目标车辆，以唤醒所述目标车辆。

[0014] 可选地，在发送所述11数据包至所述车端NFC模块之后，还包括：接收所述车端NFC模块校验所述11数据包失败后发送的11数据失败包；从所述1数据失败包中获取失败原因，并根据所述失败原因构造所述第一配对认证数据包。

[0015] 本申请第三方面实施例提供一种车辆，包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序，以实现如上述实施例所述的NFC车钥匙认证方法。

[0016] 本申请第四方面实施例提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行，以用于实现如上述实施例所述的NFC车钥匙认证方法。

[0017] 由此，通过接收车端NFC模块发出的SELECT AID，并在SELECT AID为目标AID时，判断当前移动终端是否存在长密码，若当前移动终端不存在长密码，则发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块发出的第一配对认证数据响应包，校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。

[0018] 本申请附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

[0019] 本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0020] 图1为根据本申请实施例提供的一种NFC车钥匙认证方法的流程图;

[0021] 图2为根据本申请一个实施例NFC车钥匙认证方法的流程图;

[0022] 图3为根据本申请实施例的NFC车钥匙认证装置的方框示意图;

[0023] 图4为根据本申请实施例的车辆的结构示意图。

具体实施方式

[0024] 下面详细描述本申请的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本申请,而不能理解为对本申请的限制。

[0025] 下面参考附图描述本申请实施例的NFC车钥匙认证方法、装置、车辆及存储介质。针对上述背景技术中心提到的车辆安全身份认证以及快速认证的问题,本申请提供了一种NFC车钥匙认证方法,在该方法中,通过接收车端NFC模块发出的SELECT AID,并在SELECT AID为目标AID时,判断当前移动终端是否存在长密码,若当前移动终端不存在长密码,则发送第一配对认证数据包至车端NFC模块,并接收车端NFC模块发出的第一配对认证数据响应包,校验第一配对认证数据响应包,并在第一配对认证数据响应包校验通过后,发送第二配对认证数据包至车端NFC模块,以在车端NFC模块对第二配对认证数据包校验通过后,发送CAN网络指令至目标车辆,唤醒目标车辆。由此,解决了车辆安全身份认证以及快速认证的问题,实现NFC手机安全地配对认证,同时可以快速认证。

[0026] 具体而言,图1为本申请实施例所提供的一种NFC车钥匙认证方法的流程示意图。

[0027] 如图1所示,该NFC车钥匙认证方法包括以下步骤:

[0028] 在步骤S101中,接收车端NFC模块发出的SELECT AID,并在SELECT AID为目标AID时,判断当前移动终端是否存在长密码。

[0029] 首先,车辆PKI(Public Key Infrastructure,公开密钥密码技术)云端生成一钥匙对,将nkey(私钥)通过车联网或者其它安全环境,刷入车端NFC认证模块,公钥用npkey标识。然后,车辆PKI系统根据NFC卡关联信息info(卡权限码+SN等信息+VIN(Vehicle Identification Number,车辆唯一识别码))用npkey做计算机签名得到令牌token,同时用安全算法HMAC(Hash-based Message Authentication Code,哈希运算消息认证码),nkey和token为参数,生成一个虚拟密码uvkey,云端将info、token、uvkey信息下发到用户NFC卡或者用户NFC手机。然后,当用户NFC手机靠近车端NFC模块,车端NFC模块发送SELECT AID的NFC标准选择应用指令,用户NFC手机判断是自己关注的AID,则检查memory上的LTK(long temp key,长密码)是否存在,如果不存在,则进入配对认证过程。

[0030] 在步骤S102中,若当前移动终端不存在长密码,则发送第一配对认证数据包至车端NFC模块,并接收车端NFC模块基于第一配对认证数据包发出的第一配对认证数据响应包。

[0031] 具体地,如果移动终端不存在长密码,则进入配对认证过程。手机NFC模块发送第一配对认证数据包,包标识符为01,包结构为“01+urand+info+token+校验码”,urand为临

时随机数，info为NFC卡关联信息、tokern为PKI系统对info数据用npkey做签名生成的散列，校验码对包前面数据字节做异或生成。车端NFC模块收到01数据包，采用私钥nkey验证token和info，取出info中的设备码和自己的设备码比较(比如车辆VIN码)，同时检查info数据结构中的SN是否在黑名单中，如果验签失败或者设备码匹配失败，则回复失败0101。车端NFC模块根据算法生成密钥nvkey，对收到urand随机数进行加密得到被加密后的数据eurand。车端NFC组织01标识的回复包，结构为“01+eurand+nrand+校验码”，nrand为自身随机数。

[0032] 在步骤S103中，校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。

[0033] 具体地，手机NFC模块利用虚拟密码uvkey解密被加密后的数据eurand，和随机数urand比较，如果正确则进行下一步，用uvkey加密车端NFC端随机数nrand，得到enrand；手机NFC利用车机NFC端随机数nrand和手机端随机数urand构造LTK，用LTK处理nrand。手机NFC发送第二配对认证数据包给车端NFC模块，结构为“02+enrand+LTK(nrand)”，车端NFC模块收到02数据包，解密enrand，和nrand比较，如果相同，则按照nrand和urand构造LTK，进一步校验LTK(nrand)；如果正确，则取出权限信息，比如可用日期是否在使用期限内，如果权限信息正确，则取出NFC卡指令，构造CAN总线可识别对应指令，发送到CAN总线，从而唤醒整车，执行CAN命令。

[0034] 可选地，在一些实施例中，在车端NFC模块对第二配对认证数据包校验通过后，还包括：接收车端NFC模块发送的基于第二配对认证数据包生成的第二配对认证数据响应包；校验第二配对认证数据响应包，并在第二配对认证数据响应包检验通过后，从第二配对认证数据响应包获取目标长密码，并将目标长密码存储在当前移动终端。

[0035] 可以理解的是，车端NFC模块将LTK和info数据存储到memory，同时会把将第二配对认证数据包的第二配对认证数据响应包用LTK处理后发送给手机NFC模块，手机NFC模块收到第二配对认证数据响应包，用LTK校验第二配对认证数据响应包，成功则将LTK保存到移动终端memory。

[0036] 可选地，在一些实施例中，上述的NFC车钥匙认证方法，还包括：若当前移动终端存在长密码，则构造11数据包，并发送11数据包至车端NFC模块；接收车端NFC模块校验11数据包通过后发送的11数据响应包；校验11数据响应包，并在11数据响应包检验通过后，从11数据响应包中获取目标长密码，并将目标长密码存储在当前移动终端。

[0037] 可选地，在一些实施例中，在发送11数据包至车端NFC模块之后，还包括：接收车端NFC模块校验11数据包失败后发送的11数据失败包；从1数据失败包中获取失败原因，并根据失败原因构造第一配对认证数据包。

[0038] 可选地，在一些实施例中，在接收车端NFC模块校验11数据包通过后发送的11数据响应包之后，还包括：发送CAN网络指令至目标车辆，以唤醒目标车辆。

[0039] 可以理解的是，如果手机端NFC模块检测到LTK存在，则发送11数据包到车端NFC模块，结构为“11+LTK_EP(urand)+LTK_CMAC(urand)+SN(Serial Number，密钥唯一识别码)+校验码”，其中，LTK_CMAC为利用LTK做key，对message做hash运算，LTK_EP为利用LTK做key，对message做加密运算。如果车端NFC模块收到11数据包，从数据报文中取出SN，根据SN到

flash取出对应的LTK，验证urand和LTK_CMAC(urand)，如果验证成功，生成新的随机数nrand，并生成回复报文，结构为“11+LTK_EP(nrand)+LTK_CMAC(nrand)+SN”。手机NFC模块收到数据，则利用自己的LTK进行验签，如果成功，根据分组密码的消息认证码算法，利用urand+nrand生成对等新的LTK保存。手机NFC模块回复12数据报文到车端NFC，表示已经正确解析到随机数。车端收到该12指令，进行执行车控指令，同时保存LTK。如果车端模块校验随机数不正确，则发出全校验指令。

[0040] 其中，本申请实施例可以采用黑名单机制，如果NFC卡遗失，通过云端下发该卡SN号到车端模块，从而限制该卡的使用。

[0041] 根据本申请实施例提出的NFC车钥匙认证方法，通过接收车端NFC模块发出的SELECT AID，并在SELECT AID为目标AID时，判断当前移动终端是否存在长密码，若当前移动终端不存在长密码，则发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块发出的第一配对认证数据响应包，校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。由此，解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。

[0042] 其次参照附图描述根据本申请实施例提出的NFC车钥匙认证装置，解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。

[0043] 图3是本申请实施例的NFC车钥匙认证装置的方框示意图。

[0044] 如图3所示，该NFC车钥匙认证装置10包括：判断模块100、第一接收模块200和第二发送模块300。

[0045] 其中，判断模块100，用于接收车端NFC模块发出的SELECT AID，并在SELECT AID为目标AID时，判断当前移动终端是否存在长密码；第一接收模块200，用于若当前移动终端不存在长密码，则发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块基于第一配对认证数据包发出的第一配对认证数据响应包；第一发送模块300，用于校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。

[0046] 可选地，在一些实施例中，在车端NFC模块对第二配对认证数据包校验通过后，第一发送模块300，具体用于：接收车端NFC模块发送的基于第二配对认证数据包生成的第二配对认证数据响应包；校验第二配对认证数据响应包，并在第二配对认证数据响应包检验通过后，从第二配对认证数据响应包获取目标长密码，并将目标长密码存储在当前移动终端。

[0047] 可选地，在一些实施例中，上述的NFC车钥匙认证装置10，还包括：第二发送模块，用于若当前移动终端存在长密码，则构造11数据包，并发送11数据包至车端NFC模块；第二接收模块，用于接收车端NFC模块校验11数据包通过后发送的11数据响应包；存储模块，用于校验11数据响应包，并在11数据响应包检验通过后，从11数据响应包中获取目标长密码，并将目标长密码存储在当前移动终端。

[0048] 可选地，在一些实施例中，在接收车端NFC模块校验11数据包通过后发送的11数据响应包之后，还包括：发送CAN网络指令至目标车辆，以唤醒目标车辆。

[0049] 可选地，在一些实施例中，在发送11数据包至车端NFC模块之后，还包括：接收车端NFC模块校验11数据包失败后发送的11数据失败包；从1数据失败包中获取失败原因，并根据失败原因构造第一配对认证数据包。

[0050] 需要说明的是，前述对NFC车钥匙认证方法实施例的解释说明也适用于该实施例的NFC车钥匙认证装置，此处不再赘述。

[0051] 根据本申请实施例提出的NFC车钥匙认证装置，通过接收车端NFC模块发出的SELECT AID，并在SELECT AID为目标AID时，判断当前移动终端是否存在长密码，若当前移动终端不存在长密码，则发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块发出的第一配对认证数据响应包，校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆。由此，解决了车辆安全身份认证以及快速认证的问题，实现NFC手机安全地配对认证，同时可以快速认证。

[0052] 图4为本申请实施例提供的车辆的结构示意图。该车辆可以包括：

[0053] 存储器401、处理器402及存储在存储器401上并可在处理器402上运行的计算机程序。

[0054] 处理器402执行程序时实现上述实施例中提供的NFC车钥匙认证方法。

[0055] 进一步地，车辆还包括：

[0056] 通信接口403，用于存储器401和处理器402之间的通信。

[0057] 存储器401，用于存放可在处理器402上运行的计算机程序。

[0058] 存储器401可能包含高速RAM存储器，也可能还包括非易失性存储器(non-volatile memory)，例如至少一个磁盘存储器。

[0059] 如果存储器401、处理器402和通信接口403独立实现，则通信接口403、存储器401和处理器402可以通过总线相互连接并完成相互间的通信。总线可以是工业标准体系结构(Industry Standard Architecture，简称为ISA)总线、外部设备互连(Peripheral Component，简称为PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture，简称为EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图4中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0060] 可选的，在具体实现上，如果存储器401、处理器402及通信接口403，集成在一块芯片上实现，则存储器401、处理器402及通信接口403可以通过内部接口完成相互间的通信。

[0061] 处理器402可能是一个中央处理器(Central Processing Unit，简称为CPU)，或者是特定集成电路(Application Specific Integrated Circuit，简称为ASIC)，或者是被配置成实施本申请实施例的一个或多个集成电路。

[0062] 本申请实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如上的NFC车钥匙认证方法。

[0063] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或N个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技

术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0064] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“N个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0065] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更N个用于实现定制逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本申请的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本申请的实施例所属技术领域的技术人员所理解。

[0066] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，可以被认为是用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，"计算机可读介质"可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或N个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0067] 应当理解，本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，N个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。如，如果用硬件来实现和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0068] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0069] 此外，在本申请各个实施例中的各功能单元可以集成在一个处理模块中，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模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0070] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请的限

制,本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。

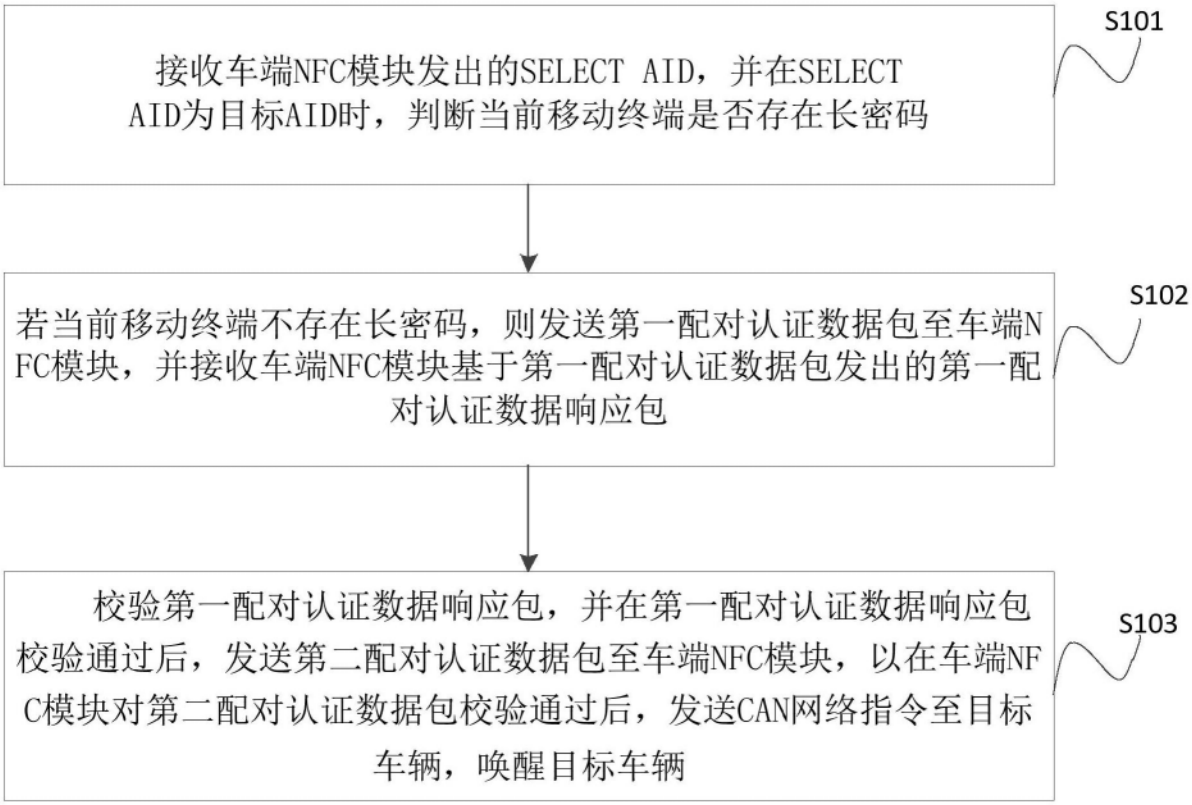

S101
接收车端NFC模块发出的SELECT AID，并在SELECT AID为目标AID时，判断当前移动终端是否存在长密码
S102
若当前移动终端不存在长密码，则发送第一配对认证数据包至车端NFC模块，并接收车端NFC模块基于第一配对认证数据包发出的第一配对认证数据响应包
S103
校验第一配对认证数据响应包，并在第一配对认证数据响应包校验通过后，发送第二配对认证数据包至车端NFC模块，以在车端NFC模块对第二配对认证数据包校验通过后，发送CAN网络指令至目标车辆，唤醒目标车辆

图1

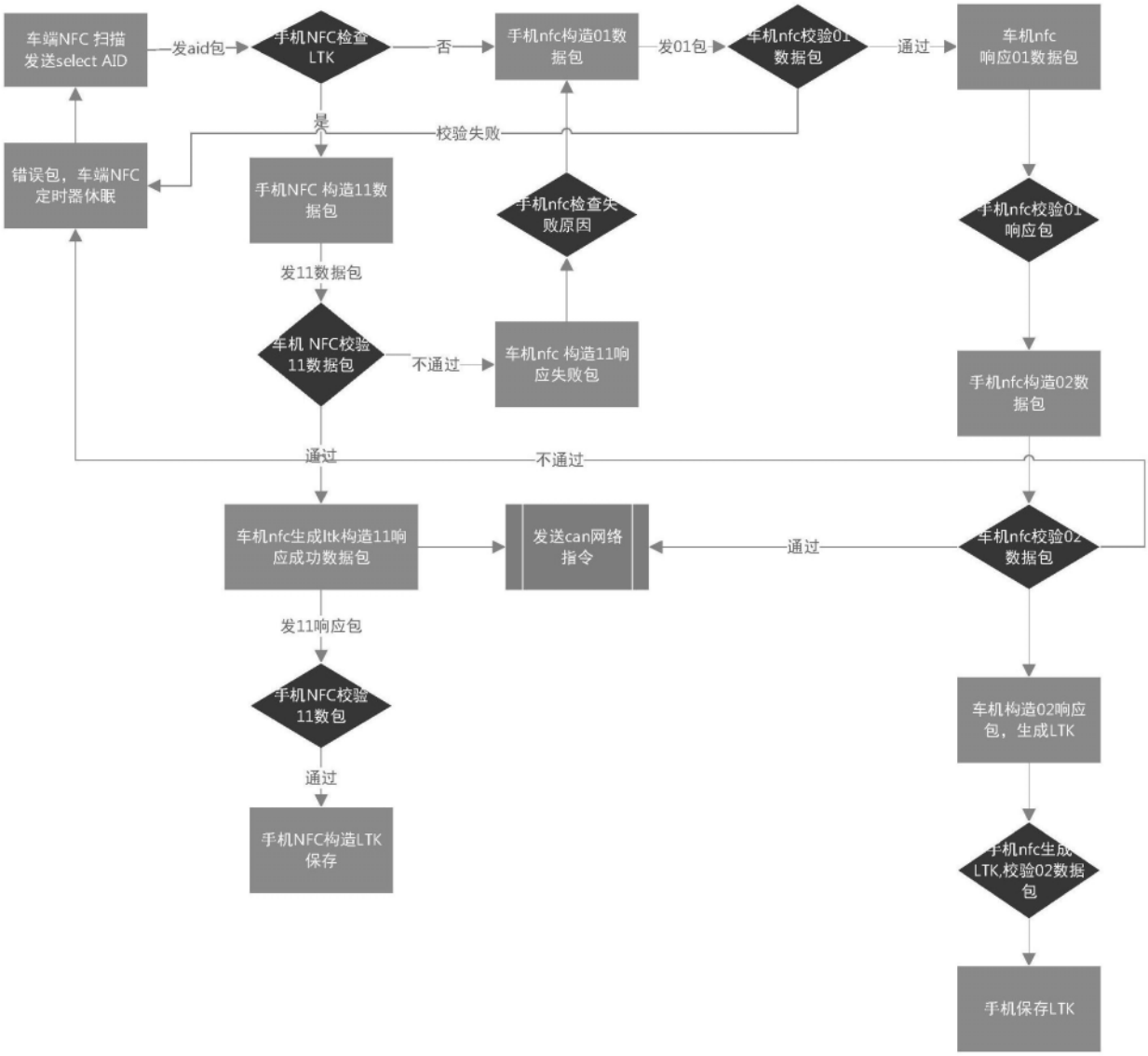

车端NFC 扫描
发送select AID
发aid包
手机NFC检查
LTK
否
手机nfc构造01数
据包
发01包
车机nfc校验01
数据包
通过
车机nfc
响应01数据包
是
校验失败
错误包，车端NFC
定时器休眠
手机NFC 构造11数
据包
手机nfc检查失
败原因
手机nfc校验01
响应包
发11数据包
车机 NFC校验
11数据包
不通过
车机nfc 构造11响
应失败包
手机nfc构造02数
据包
通过
不通过
车机nfc生成ltk构造11响
应成功数据包
发送can网络
指令
通过
车机nfc校验02
数据包
发11响应包
手机NFC校验
11数包
车机构造02响应
包，生成LTK
通过
手机NFC构造LTK
保存
手机nfc生成
LTK,校验02数据
包
手机保存LTK

图2

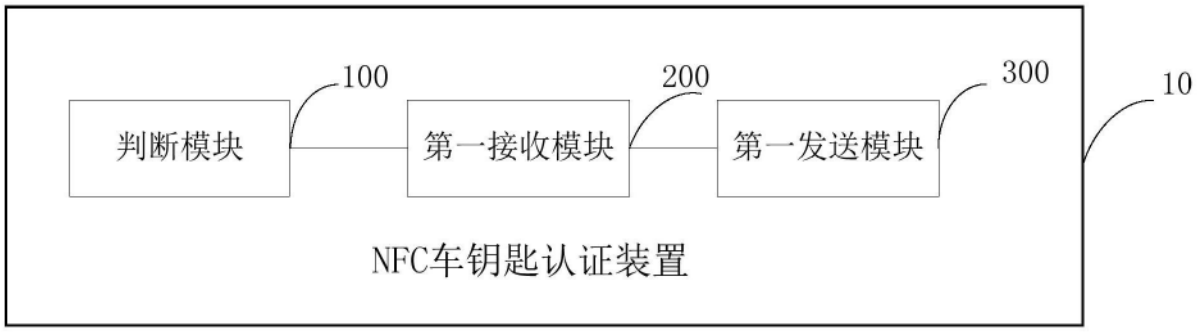

100
200
300
10
判断模块
第一接收模块
第一发送模块
NFC车钥匙认证装置

图3

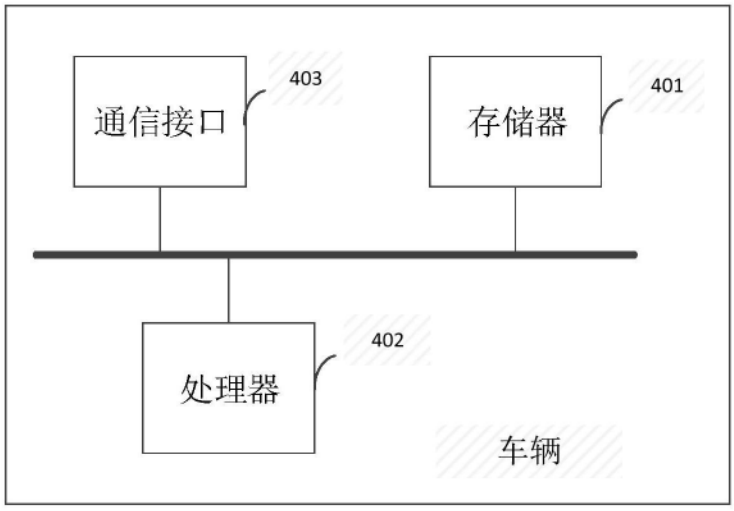


图4