(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111845624 B
(45)授权公告日 2022.12.09

(21)申请号 202010725356.7

(22)申请日 2020.07.24

(65)同一申请的已公布的文献号
申请公布号 CN 111845624 A

(43)申请公布日 2020.10.30

(73)专利权人 重庆长安汽车股份有限公司
地址 400023 重庆市江北区建新东路260号

(72)发明人 刘平 谭成宇 张鹏 王晓伟
罗薇 袁野

(74)专利代理机构 重庆华科专利事务所 50123
专利代理师 康海燕

(51)Int.Cl.
B60R 25/10(2013.01)
B60R 25/20(2013.01)
H04W 4/48(2018.01)
H04W 12/00(2021.01)
H04W 12/06(2021.01)
H04W 12/10(2021.01)

审查员 袁娇娇

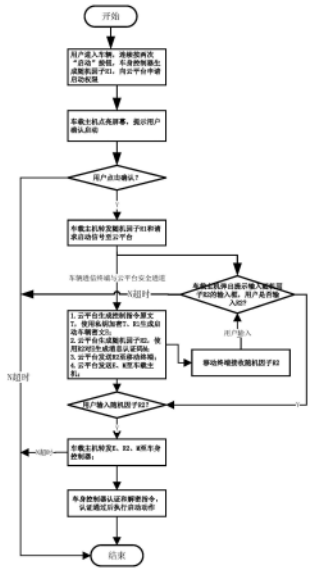
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种无钥匙启动车辆的方法

(57)摘要

本方案涉及一种无钥匙启动车辆的方法，以低成本、高安全性实现车辆启动。包括：BCM接收用户输入信号生成随机因子R1，发送启动请求信号至车机；车机点亮屏幕，请求用户确认，若车机收到确认信号，转发启动请求信号至云平台；云平台生成控制指令原文T和随机因子R2，使用非对称加密算法的私钥对T、R1加密生成E，使用R2对E进行单向散列算法生成M；发送E、M至车机，发送R2至移动终端；若车机收到R2，转发R2、E、M至BCM；BCM使用R2对E、进行单向散列算法生成M'；若M'与M相同，则密文E完整性校验通过；BCM使用非对称密码算法的公钥解密E得到T、R1'；若R1'与R1相同且控制指令原文T各项参数满足条件，则BCM根据T执行启动车辆。



CN 111845624 B

1.一种无钥匙启动车辆的方法,其特征在于,包括以下步骤:

步骤S1:车身控制器(1)接收用户输入的激活启动功能信号,基于所激活启动功能信号生成随机因子R1,并将携带有所述随机因子R1的启动请求信号发送至车载主机;

步骤S2:车载主机(2)基于所述启动请求信号,点亮车载主机(2)屏幕,并输出提示用户进行确认激活车辆启动的信息,若车载主机(2)在第一设定时间内接收到用户输入的确认信号,则执行步骤S3;否则,结束流程;

步骤S3: 车载主机(2)使用预先与云平台(3)建立的安全通道将所述启动请求信号转发至云平台(3);在完成所述启动请求信号转发后,所述车载主机(2)输出提示用户输入随机因子R2的提示窗口;

步骤S4:云平台(3)基于所述启动请求信号生成控制指令原文T和随机因子R2,并使用非对称加密算法的私钥对所述控制指令原文T和随机因子R1加密生成密文E,使用随机因子R2对密文E进行单向散列算法生成消息认证码M;

步骤S5:云平台(3)将密文E和消息认证码M发送至车载主机(2),并将随机因子R2发送至移动终端(4);

步骤S6:若车载主机(2)在输出提示窗口后的第二设定时间内接收到用户输入的随机因子R2,则将随机因子R2、密文E和消息认证码M转发至车身控制器(1);否则,结束流程;

步骤S7:车身控制器(1)使用车载主机(2)转发的随机因子R2对密文E进行单向散列算法生成消息认证码M';若判断出消息认证码M'与消息认证码M相同,则确定密文E的完整性校验通过,执行步骤S8;否则,结束流程;

步骤S8:车身控制器(1)使用非对称密码算法的公钥解密接收到的密文E,得到控制指令原文T、随机因子R1';若车身控制器(1)判断出随机因子R1'与随机因子R1相同且控制指令原文T各项参数满足条件,则执行步骤S9;否则,结束流程;

步骤S9:车身控制器(1)根据解密后获得的控制指令原文T的内容执行启动车辆;然后,结束流程。

一种无钥匙启动车辆的方法

技术领域

[0001] 本发明用于车辆进出系统技术领域，具体涉及一种无钥匙启动车辆的方法。

背景技术

[0002] 随着移动网络技术的发展，车辆配置车载移动通信终端的比例越来越高，因此通过移动终端控制车辆的功能逐渐成为一种趋势，如远程车况查询、远程控制车辆开启空调、远程寻车、解闭锁等功能。云平台作为车载移动通信终端与移动通信终端相互通讯的桥梁，其不仅承担了建立双方通信通道的功能，还需对车载移动通信终端和移动终端进行双向身份认证。车载移动通信终端、云平台由整车厂开发实现，整车厂可以在车载移动通信终端中预置安全证书与云平台进行双向身份认证和建立安全通道，并且该证书每个车辆均不相同。然而，移动终端不受整车厂掌控，且移动终端生产厂商种类繁多，无法事先预置与整车厂云平台的安全证书，使得无法直接进行双向身份认证。

[0003] 移动终端通过输入账号和密码登录APP，该APP能够与整车厂云平台通信，账号和密码作为与云平台认证的凭据，由于云平台与APP之间没有可信的安全通道，且不能安全保存账号和密码，导致账号和密码的信息安全风险极高，为避免车辆被盗走的风险，大多数车辆不支持不带钥匙的情况下控制车辆启动并能驾驶的功能。

[0004] 一种基于识别密码的电动车启动控制方法(201310022551.3)和一种汽车启动系统(201710309083.6)，均提供了一种事先在车内预置或设置密码的方式，用户输入同样的密码进行比对的方法启动车辆。其存在两方面的问题，其一，无法进行身份认证，上述专利中，密码即代表用户身份，若密码被他人窃取后，他人就能获取车主的权限；其二，存在较大的密码泄露风险，密码在驻留过的地方均留有痕迹，容易被黑客进行远程破解。上述专利中实现的信息安全方法风险较大，容易出现盗车风险。

发明内容

[0005] 本发明的目的是提供一种无钥匙启动车辆的方法，其可以以低成本、高安全性实现控制车辆启动。

[0006] 本发明提供了一种无钥匙启动车辆的方法，其特征在于，包括以下步骤：

[0007] 步骤S1：车身控制器接收用户输入的激活启动功能信号，基于所激活启动功能信号生成随机因子R1，并将携带有所述随机因子R1的启动请求信号发送至车载主机；

[0008] 步骤S2:车载主机基于所述启动请求信号，点亮车载主机屏幕，并输出提示用户进行确认激活车辆启动的信息，若车载主机在第一设定时间内接收到用户输入的确认信号，则执行步骤S3；否则，结束流程；

[0009] 步骤S3: 车载主机使用预先与云平台建立的安全通道将所述启动请求信号转发至云平台；在完成所述启动请求信号转发后，所述车载主机输出提示用户输入随机因子R2的提示窗口；

[0010] 步骤S4:云平台基于所述启动请求信号生成控制指令原文T和随机因子R2，并使用

非对称加密算法的私钥对所述控制指令原文T和随机因子R1加密生成密文E，使用随机因子R2对密文E进行单向散列算法生成消息认证码M；

[0011] 步骤S5：云平台将密文E和消息认证码M发送至车载主机，并将随机因子R2发送至移动终端；

[0012] 步骤S6：若车载主机在输出提示窗口后的第二设定时间内接收到用户输入的随机因子R2，则将随机因子R2、密文E和消息认证码M转发至车身控制器；否则，结束流程；

[0013] 步骤S7：车身控制器使用车载主机转发的随机因子R2对密文E进行单向散列算法生成消息认证码M'；若判断出消息认证码M'与消息认证码M相同，则确定密文E的完整性校验通过，执行步骤S8；否则，结束流程；

[0014] 步骤S8：车身控制器使用非对称密码算法的公钥解密接收到的密文E，得到控制指令原文T、随机因子R1'；若车身控制器判断出随机因子R1'与随机因子R1相同且控制指令原文T各项参数满足条件，则执行步骤S9；否则，结束流程；

[0015] 步骤S9：车身控制器根据解密后获得的控制指令原文T的内容执行启动车辆；然后，结束流程。

[0016] 本发明具有以下优点：

[0017] (1)基于配备有车载通信终端的车辆，仅需要在车辆出厂前将非对称公钥预置到车身控制器，公钥仅需要做不被篡改的信息安全措施，即可实现该功能，成本低；

[0018] (2)对同一车型，预置到车身控制器的公钥可以是相同的，降低生产和维护成本；

[0019] (3)所述的移动终端，可以是任意能够代表用户身份的设备，如插有用户实名认证的SIM卡的智能手表或手机，微信实名认证账户等，在移动终端中，未存储有私钥，而是将私钥存储在车和云平台上，他人窃取破译私钥难度大，且成本极高，提高了车辆的防盗性能，同时移动终端不需要增加特别的信息安全防护措施，实现成本低。

[0020] (4)本发明可作为低成本的备用启动车辆的方案，在车辆钥匙没电或车辆无线接收器工作异常的情况下，用户可以通过机械钥匙解锁进入车辆后，使用本发明启动车辆。

附图说明

[0021] 图1为本发明的结构框图；

[0022] 图2为本发明的密文E和消息认证码M的加密原理图；

[0023] 图3为本发明的密文E和消息认证码M的解密原理图；

[0024] 图4为本发明的方法流程图；

[0025] 图中：1、车身控制器，2、车载主机，3、云平台，4、移动终端。

具体实施方式

[0026] 下面结合附图对本发明作进一步说明。

[0027] 如图4，本发明提供了一种无钥匙启动车辆的方法，该方法包括：

[0028] 步骤S1：用户通过移动终端发送解锁命令或通过机械钥匙解锁车辆进入车辆后，连续按压两次车辆上搭载的“启动”按钮，激活启动功能，车身控制器BCM1接收用户连续两次按压“启动”按钮的激活信号，然后，通过真随机数生成器或计时器生成随机因子R1，并发送携带有所生成的随机因子R1的启动请求信号至车载主机2。

[0029] 步骤S2:车载主机2接收到车身控制器BCM1发送的启动请求信号后,点亮车载主机2的屏幕,并通过车载主机2的显示屏幕输出提示用户进行确认激活车辆启动的显示信息,若用户在第一设定时间(如5s、10s等时间)内点击“确认”图标,则执行步骤S3,若否(即用户点击拒绝或取消或者未在第一设定时间内操作),则结束流程。

[0030] 步骤S3:车载主机2使用与云平台3预先建立的安全通道(车辆的T-box终端与云平台建立的通道)转发携带有随机因子R1的启动请求信号至云平台3;然后,车载主机2的屏幕上显示提示用户输入随机因子R2的窗口。

[0031] 步骤S4:云平台3基于与车身控制器BCM1之间预先定义的控制指令格式和内容,生成控制指令原文T;同时,云平台3使用非对称加密算法的私钥对控制指令原文T、随机因子R1加密生成密文E,再基于真随机数生成器生成随机因子R2,最后使用随机因子R2对密文E进行单向散列算法生成消息认证码M。

[0032] 步骤S5:云平台3将密文E、消息认证码M发送至车载主机2,将随机因子R2发送至移动终端4;在步骤S5中,云平台3通过短信验证码的方式将该随机因子R2发送至移动终端4,对于移动终端4来说,无需下载APP,也无需进行数据处理,仅需要接收一条短信提示信息即可。由于在移动终端4、车辆端无需存储非对称密码算法的私钥或对称密码算法的对称密钥;而是将非对称密码算法的私钥等敏感信息存储到云平台3上,相对来说,不法分子很难破解存储在云平台3的私钥和密钥,极有利于车辆的防盗。

[0033] 步骤S6:车载主机2等待用户输入随机因子R2,若车载主机2从显示提示用户输入随机因子R2的显示窗口后第二设定时间(如10分钟内)内接收到随机因子R2,将随机因子R2、控制指令密文E和消息认证码M转发至车身控制器BCM1,执行步骤S7,若否,则结束流程。

[0034] 步骤S7:车身控制器BCM1使用R2对接收到的密文E进行单向散列算法生成消息认证码M’,若消息认证码M’与消息认证码M相同,则确定密文E的完整性校验通过,执行步骤S8,若否,则结束流程。

[0035] 步骤S8:车身控制器BCM1使用非对称密码算法的公钥验签和解密密文E,得到控制指令原文T和随机因子R1’,若随机因子R1’与随机因子R1相同,且控制指令原文T各项参数满足条件,则执行步骤S9,若否,则结束流程;

[0036] 步骤S9:车身控制器BCM1根据控制指令原文T的内容执行指令,本例为启动车辆,结束流程。

[0037] 如图1所示,本发明所述的一种基于随机因子实现启动车辆的信息安全设计方法,该方法应用于一种无钥匙启动车辆的系统,其中,该系统包括:包括车辆、云平台3、移动终端4;其中:所述的车辆包含车身控制器BCM1、车载主机2。车载主机2和车身控制器BCM1之间通过CAN网络连接,车载主机2通过移动网络和云平台3连接,移动终端4和云平台3通过移动网络连接。

[0038] 本实施例中,所述的车身控制器BCM1被配置为,检测启动车辆请求,本实施例中检测启动车辆请求为用户连续按两次启动按钮,向车载主机2发送请求启动车辆的启动请求信号,启动请求信号中包含有车身控制器BCM1基于真随机码生成器生成的随机因子R1,在发起启动请求信号后k1分钟内等待车辆启动命令和随机因子R2,本实时例中k1为10分钟,接收到命令和随机因子R2后进行验证和解密,成功后执行启动车辆命令。车身控制器1在车辆出厂前预置非对称密钥,且具有非对称解密算法、存储非对称公钥且不能被篡改的能力,

验证控制指令的合法性。

[0039] 本实施例中，所述的车载主机2被配置为，建立和保持与云平台的安全通信，接收车身控制器BCM的启动请求信号，并弹出用户确认界面和输入随机因子R2的界面，同时将启动请求信号发送到云平台，发送命令后等待云平台下发启动车辆的命令和用户输入随机因子R2k2分钟，本实施例中，k2为10分钟，车载主机1接收到命令和随机因子R2后，转发至车身控制器BCM1。车载主机1在出厂前预置有证书，与云平台3进行身份认证和安全通信。

[0040] 本实施例中，所述的云平台3被配置为，接收到车载主机2发送的请求启动信号后，组装控制指令原文T、以及加密的密文E和消息认证码M，并将其下发到车载主机2；同时，云平台将生成的随机因子R2，下发到移动终端4。云平台3为根可信平台，具有非对称加密、安全存储非对称私钥且不能被其他设备获取的能力，同时与车载主机2进行身份认证和安全通信。

[0041] 本实施例中，所述的移动终端4被配置为，显示和接收云平台3下发的随机因子R2，本实施例中，所述的移动终端4为插有用户实名认证SIM卡的手机，通过短信的方式下发随机因子R2到插有SIM卡的手机；

[0042] 本实施例中，随机因子R2均为6位随机数。

[0043] 本实施例中，信号加密及消息认证码生成原理如附图2所示，云平台3被认为是可信的平台，采用非对称加密算法的私钥能够被安全保存且不会被其他装置获取，同时加密和消息认证码生成过程中加入了车身控制器BCM1的随机因子R1和云平台3的随机因子R2，随机因子R2通过第三方渠道(短信)发送给用户。

[0044] 本实施例中，密文解密及消息认证码验证校验原理如附图3所示，用户将随机因子R2输入到车载主机2并转发到车身控制器BCM1后，车身控制器BCM1才能校验指令密文，校验完成后正确解密指令密文才会执行启动车辆命令。

[0045] 本实施例的上述方法，在车辆启动时，需要与云平台预先认证通过的移动终端接收云平台下发的随机因子R2，并需要用户手动输入随机因子R2到车载主机2，进一步由车身控制器BCM1进行认证，在认证通过后才执行车辆启动动作。该方案，需要车，人，移动终端和云平台四个主体共同参与，才可实现车辆的无钥匙启动。并且，由于在移动终端、车辆端无需存储非对称密码算法的私钥或对称密码算法的对称密钥；而是将非对称密码算法的私钥等敏感信息存储到云平台上，车端仅需要安全存储不敏感的非对称算法的公钥，即便被他人知道也无安全风险，相对来说，不法分子很难破解存储在云平台端的私钥和密钥，极有利于车辆的防盗。

[0046] 本实施例中，控制指令原文T事先由云平台3和BCM1按相同的格式和内容定义，其必须包含执行动作编码(如启动车辆、车辆上电等)、时间戳(云平台3组装原文时的时间，BCM1必须判断时间戳大于上次执行命令的时间戳，避免重放攻击)，车端随机因子R1(BCM1通过R1判断该启动请求是BCM1自己请求的)，以及其他自定义的内容。

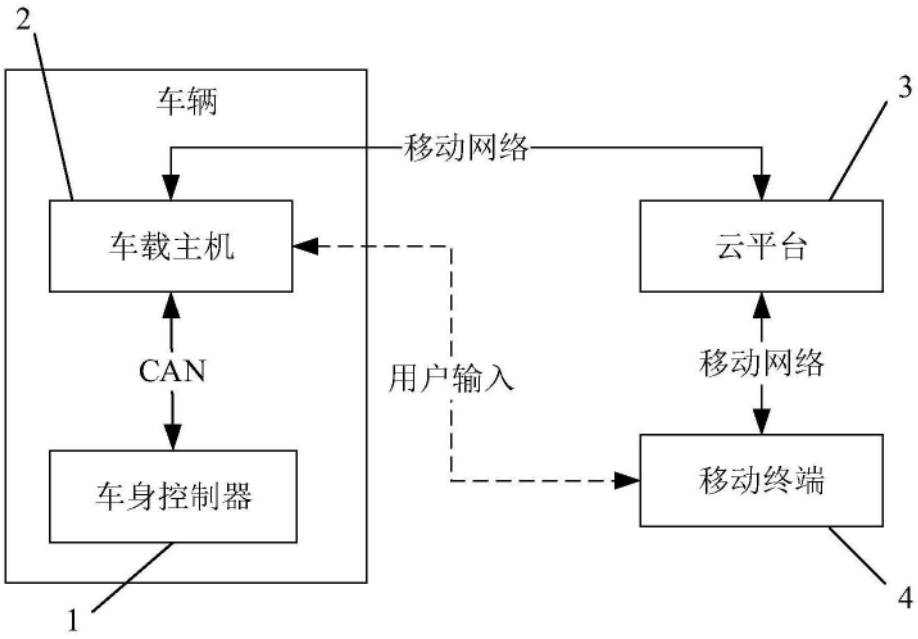

2
车辆
移动网络
3
车载主机
云平台
CAN
用户输入
移动网络
车身控制器
移动终端
1
4

图1

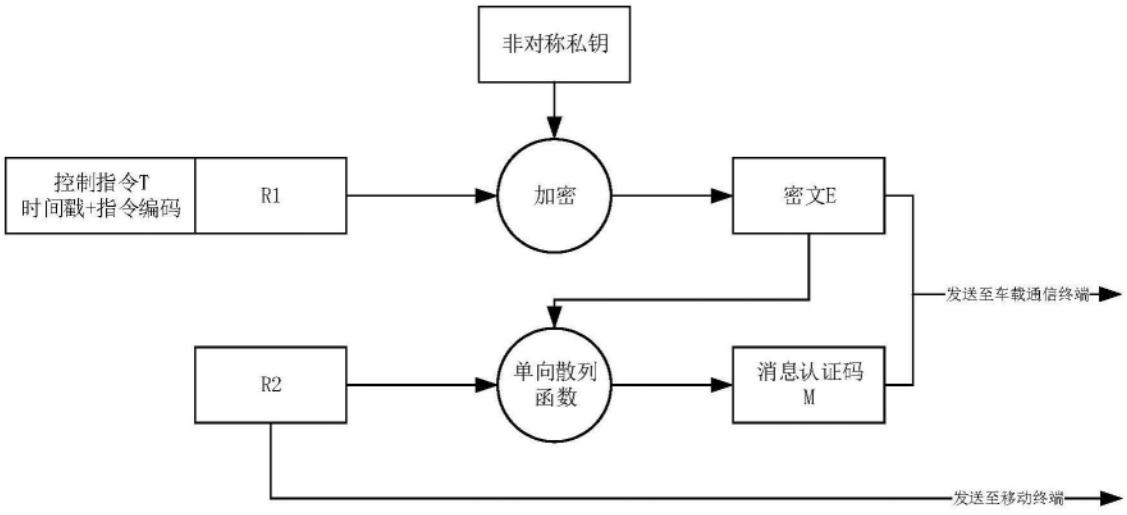

非对称私钥
控制指令T
时间戳+指令编码
R1
加密
密文E
发送至车载通信终端
R2
单向散列
函数
消息认证码
M
发送至移动终端

图2

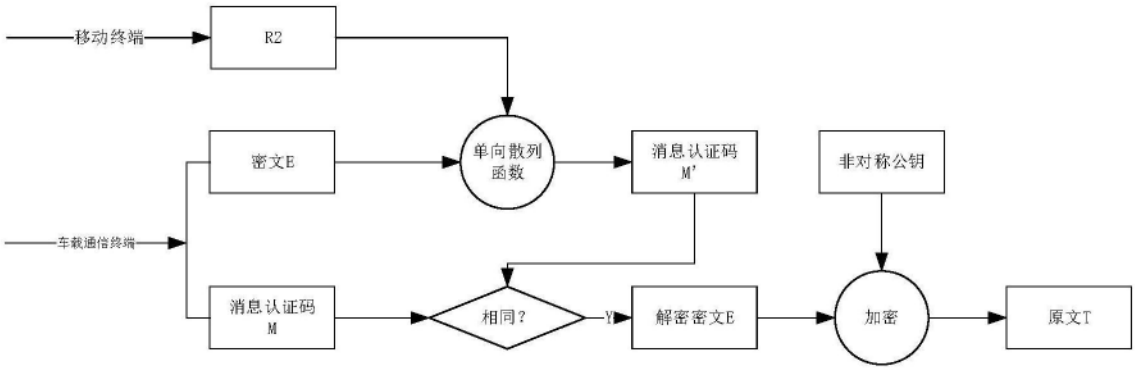

移动终端
R2
密文E
单向散列函数
消息认证码M'
非对称公钥
车载通信终端
消息认证码M
相同?
Y
解密密文E
加密
原文T

图3

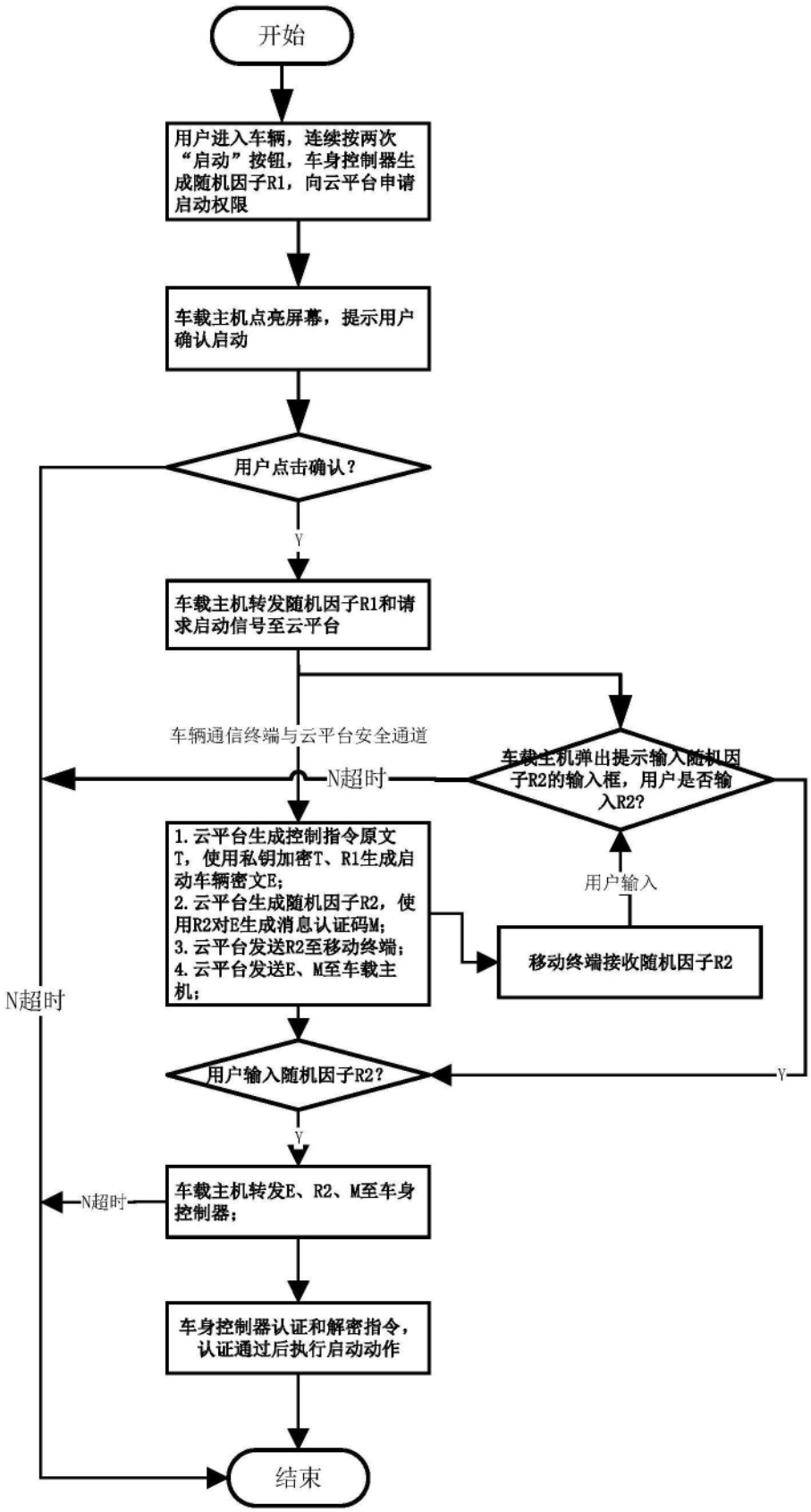

开始
用户进入车辆，连续按两次“启动”按钮，车身控制器生成随机因子R1，向云平台申请启动权限
车载主机点亮屏幕，提示用户确认启动
用户点击确认？
Y
车载主机转发随机因子R1和请求启动信号至云平台
车辆通信终端与云平台安全通道
N超时
车载主机弹出提示输入随机因子R2的输入框，用户是否输入R2?
用户输入
1.云平台生成控制指令原文T，使用私钥加密T、R1生成启动车辆密文E；
2.云平台生成随机因子R2，使用R2对E生成消息认证码M；
3.云平台发送R2至移动终端；
4.云平台发送E、M至车载主机；
移动终端接收随机因子R2
N超时
用户输入随机因子R2?
Y
Y
N超时
车载主机转发E、R2、M至车身控制器；
车身控制器认证和解密指令，认证通过后执行启动动作
结束

图4