(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 111083696 A
(43)申请公布日 2020.04.28

(21)申请号 201911413942.1

(22)申请日 2019.12.31

(71)申请人 智车优行科技(北京)有限公司
地址 100020 北京市朝阳区北三环北路27号嘉铭中心B座2层

(72)发明人 赵江 韦自升

(74)专利代理机构 北京思源智汇知识产权代理有限公司 11657
代理人 王晓多

(51)Int.Cl.
H04W 12/00(2009.01)
H04W 12/02(2009.01)
H04W 12/06(2009.01)

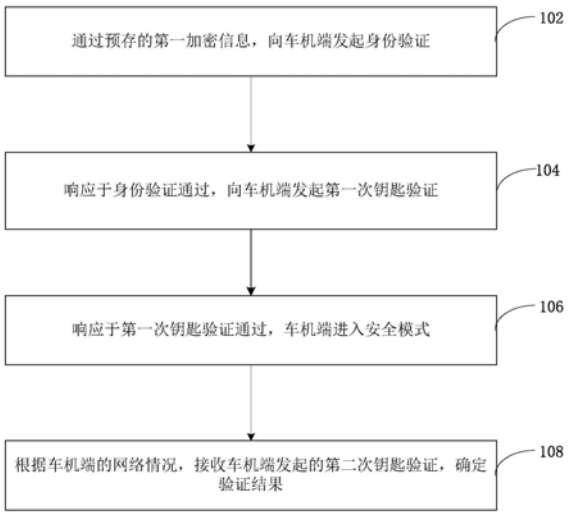
权利要求书2页 说明书19页 附图5页

(54)发明名称

通信验证方法和系统、移动终端、车机端

(57)摘要

本申请实施例公开了一种通信验证方法和系统、移动终端、车机端，其中，方法包括：通过预存的第一加密信息，向车机端发起身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到；响应于所述身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，所述车机端进入安全模式；根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果，本实施例通过身份验证以及两次钥匙验证提高了车机端的安全性，防止由于身份信息泄露或数据在传输过程中被截取篡改。



CN 111083696 A

1.一种通信验证方法,其特征在于,应用于移动终端,包括:

通过预存的第一加密信息,向车机端发起身份验证;其中,所述第一加密信息为车机身份数字证书经过第一私钥加密得到;

响应于所述身份验证通过,向所述车机端发起第一次钥匙验证;

响应于所述第一次钥匙验证通过,所述车机端进入安全模式;

根据所述车机端的网络情况,接收所述车机端发起的第二次钥匙验证,确定验证结果。

2.根据权利要求1所述的方法,其特征在于,所述通过预存的第一加密信息,向车机端发起身份验证,包括:

将所述第一加密信息发送给所述车机端,通过所述车机端根据所述第一加密信息对所述移动终端的身份进行验证;

接收所述车机端反馈预存在所述车机端的第二加密信息;其中,所述第二加密信息为终端数字身份证书经过第二私钥加密得到;

通过预存的第二公钥对所述第二加密信息进行解密,根据得到的终端数字身份证书确认所述车机端的身份。

3.根据权利要求2所述的方法,其特征在于,所述通过预存的第一加密信息,向车机端发起身份验证的同时,还包括:

对接收的所述第二加密信息进行解密,获得所述车机端确认的通信加密方法和通信加密密钥;以所述通信加密方法和所述通信加密密钥加密后续与所述车机端之间的通信信息。

4.根据权利要求1-3任一所述的方法,其特征在于,所述响应于所述身份验证通过,向所述车机端发起钥匙信息验证,包括:

响应于所述身份验证通过,基于上一次钥匙验证使用的第三历史加密信息对应的历史序列号确定当前序列号;

基于所述当前序列号确定本次通信的第三加密信息;其中,所述第三加密信息为钥匙信息证书经过第三公钥加密得到;

将所述第三加密信息发送到所述车机端,所述车机端对所述第三加密信息进行验证,实现第一次钥匙验证。

5.根据权利要求4所述的方法,其特征在于,在通过预存的第一加密信息,向车机端发起身份验证之前,还包括:

确定所述移动终端中是否包括历史加密信息;

响应于包括所述历史加密信息,确定所述历史加密信息是否过期,如果过期,向云端请求更新所述历史加密信息;否则,将所述历史加密信息作为所述第三加密信息;

响应于不包括所述历史加密信息,向所述云端请求获取所述第三加密信息并存储。

6.根据权利要求5所述的方法,其特征在于,所述向所述云端请求获取所述第三加密信息并存储,包括:

向所述云端发送信息请求;

接收所述云端根据所述信息请求反馈的所述第三加密信息;

将所述第三加密信息存入安全元件中。

7.一种通信验证方法,其特征在于,应用于车机端,包括:

接收移动终端发送的第一加密信息，基于所述第一加密信息和预存的第二加密信息进行身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到，所述第二加密信息为所述终端数字身份证书经过第二私钥加密得到；

响应于所述身份验证通过，接收所述移动终端发起的第一次钥匙验证；

响应于所述第一次钥匙验证通过，进入安全模式；

根据网络情况，发起第二次钥匙验证，确定验证结果。

8.一种移动终端，其特征在于，包括：

身份验证模块，用于通过预存的第一加密信息，向车机端发起身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到；

第一钥匙验证模块，用于响应于所述身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，所述车机端进入安全模式；

第二钥匙验证模块，用于根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果。

9.一种车机端，其特征在于，包括：

身份验证模块，用于接收移动终端发送的第一加密信息，基于所述第一加密信息和预存的第二加密信息进行身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到，所述第二加密信息为所述终端数字身份证书经过第二私钥加密得到；

第一钥匙验证模块，用于响应于所述身份验证通过，接收所述移动终端发起的第一次钥匙验证；响应于所述第一次钥匙验证通过，进入安全模式；

第二钥匙验证模块，用于根据网络情况，发起第二次钥匙验证，确定验证结果。

10.一种通信验证系统，其特征在于，包括：

如上述权利要求8所述的移动终端和如上述权利要求9所述的车机端。

通信验证方法和系统、移动终端、车机端

技术领域

[0001] 本申请涉及通信验证技术，尤其是一种通信验证方法和系统、移动终端、车机端。

背景技术

[0002] 随着互联网、人工智能、无线网络和云计算、大数据等技术的应用，今天的汽车的智能化、联网化程度越来越高，汽车已经变成名副其实的万物互联时代接入网络的智能终端设备。

[0003] 目前大部分的汽车都有电子系统，电子控制单元通过车内局域网连接，并同时连接到外部网络(比如4G和5G网络)，以实现丰富多样的汽车服务，比如车联网和自动驾驶；技术的发展推动了产品的更新，进入系统由原先的机械钥匙变为遥控系统，再到移动智能终端成为车联网标配，具备远程开启空调、门锁，远程启动车辆等功能；移动智能终端的安全间接影响车联网的安全。

发明内容

[0004] 本申请实施例提供的一种通信验证技术。

[0005] 根据本申请实施例的一个方面，提供的一种通信验证方法，应用于移动终端，包括：

[0006] 通过预存的第一加密信息，向车机端发起身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到；

[0007] 响应于所述身份验证通过，向所述车机端发起第一次钥匙验证；

[0008] 响应于所述第一次钥匙验证通过，所述车机端进入安全模式；

[0009] 根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果。

[0010] 可选地，所述通过预存的第一加密信息，向车机端发起身份验证，包括：

[0011] 将所述第一加密信息发送给所述车机端，通过所述车机端根据所述第一加密信息对所述移动终端的身份进行验证；

[0012] 接收所述车机端反馈预存在所述车机端的第二加密信息；其中，所述第二加密信息为终端数字身份证书经过第二私钥加密得到；

[0013] 通过预存的第二公钥对所述第二加密信息进行解密，根据得到的终端数字身份证书确认所述车机端的身份。

[0014] 可选地，所述通过预存的第一加密信息，向车机端发起身份验证的同时，还包括：

[0015] 对接收的所述第二加密信息进行解密，获得所述车机端确认的通信加密方法和通信加密密钥；以所述通信加密方法和所述通信加密密钥加密后续与所述车机端之间的通信信息。

[0016] 可选地，所述响应于所述身份验证通过，向所述车机端发起钥匙信息验证，包括：

[0017] 响应于所述身份验证通过，基于上一次钥匙验证使用的第三历史加密信息对应的

历史序列号确定当前序列号；

[0018] 基于所述当前序列号确定本次通信的第三加密信息；其中，所述第三加密信息为钥匙信息证书经过第三公钥加密得到；

[0019] 将所述第三加密信息发送到所述车机端，所述车机端对所述第三加密信息进行验证，实现第一次钥匙验证。

[0020] 可选地，在通过预存的第一加密信息，向车机端发起身份验证之前，还包括：

[0021] 确定所述移动终端中是否包括历史加密信息；

[0022] 响应于包括所述历史加密信息，确定所述历史加密信息是否过期，如果过期，向云端请求更新所述历史加密信息；否则，将所述历史加密信息作为所述第三加密信息；

[0023] 响应于不包括所述历史加密信息，向所述云端请求获取所述第三加密信息并存储。

[0024] 可选地，所述向所述云端请求获取所述第三加密信息并存储，包括：

[0025] 向所述云端发送信息请求；

[0026] 接收所述云端根据所述信息请求反馈的所述第三加密信息；

[0027] 将所述第三加密信息存入安全元件中。

[0028] 可选地，所述车机端的网络情况包括：网络正常情况和弱网络情况；

[0029] 所述根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果，包括：

[0030] 响应于所述车机端的网络情况为所述网络正常情况，通过云端实现所述车机端与所述移动终端的第二次钥匙验证；

[0031] 响应于所述车机端的网络情况为所述弱网络情况，通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证。

[0032] 可选地，所述通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证，包括：

[0033] 向通信服务端发送所述车机端反馈的验证请求，接收所述通信服务端根据所述验证请求反馈的第一验证码；

[0034] 将所述第一验证码发送到所述车机端，通过所述车机端实现所述第二次钥匙验证。

[0035] 可选地，所述将所述第一验证码发送到所述车机端，包括：

[0036] 将所述第一验证码通过所述通信加密密钥进行加密得到加密验证码；

[0037] 将所述加密验证码发送到所述车机端。

[0038] 可选地，还包括：

[0039] 响应于所述验证结果为通过验证，控制所述车机端；

[0040] 响应于所述验证结果为未通过验证，所述车机端进入安全模式，所述车机端发出提示信息。

[0041] 根据本申请实施例的另一方面，提供的一种通信验证方法，应用于车机端，包括：

[0042] 接收移动终端发送的第一加密信息，基于所述第一加密信息和预存的第二加密信息进行身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到，所述第二加密信息为所述终端数字身份证书经过第二私钥加密得到；

[0043] 响应于所述身份验证通过，接收所述移动终端发起的第一次钥匙验证；

[0044] 响应于所述第一次钥匙验证通过，进入安全模式；

[0045] 根据网络情况，发起第二次钥匙验证，确定验证结果。

[0046] 可选地，所述接收移动终端发送的第一加密信息，基于所述第一加密信息进行身份验证，包括：

[0047] 接收所述移动终端发送的所述第一加密信息，根据预存的第一公钥对所述第一加密信息进行解密，根据解密得到车机身份数字证书确认所述移动终端的身份；

[0048] 响应于所述移动终端的身份合法，向所述移动终端发送第二加密信息到所述移动终端，所述移动终端根据所述第二加密信息对所述车机端的身份进行验证。

[0049] 可选地，所述接收移动终端发送的第一加密信息，基于所述第一加密信息和预存的第二加密信息进行身份验证的同时，还包括：

[0050] 对所述第一加密信息进行解密，获得所述移动终端确认的通信加密方法和通信加密密钥；以所述通信加密方法和所述通信加密密钥加密后续与所述移动终端之间的通信信息。

[0051] 可选地，所述响应于所述身份验证通过，接收所述移动终端发起的第一次钥匙验证，包括：

[0052] 接收所述移动终端发送的第三加密信息并利用预存的第三私钥进行解密，得到钥匙信息证书；其中，所述第三加密信息为钥匙信息证书经过第三公钥加密得到；

[0053] 对所述钥匙信息证书进行验证，实现第一次钥匙验证。

[0054] 可选地，所述钥匙信息证书中包括：通过所述第三公钥加密的第一钥匙有效时间、通过所述第三公钥加密的私钥索引信息、以及通过第四私钥加密的第二钥匙有效时间和钥匙信息；其中，每个所述私钥索引信息对应一个第四公钥；

[0055] 所述对所述钥匙信息证书进行验证，包括：

[0056] 通过所述第三公钥解密获得所述钥匙信息证书中的所述第一钥匙有效时间和所述私钥索引信息；

[0057] 通过所述私钥索引信息查找获得所述第四公钥；

[0058] 通过第四公钥对所述钥匙信息证书进一步解密，获得所述第二钥匙有效时间和所述钥匙信息；

[0059] 基于所述第一钥匙有效时间和所述第二钥匙有效时间对所述钥匙信息进行验证。

[0060] 可选地，所述基于所述第一钥匙有效时间和所述第二钥匙有效时间对所述钥匙信息进行验证，包括：

[0061] 比对所述第一钥匙有效时间与所述第二钥匙有效时间；

[0062] 响应于所述第一钥匙有效时间与所述第二钥匙有效时间相等，根据所述第二钥匙有效时间和当前时间，确认所述钥匙信息是否在有效时间内；

[0063] 响应于所述钥匙信息在有效时间内确认验证通过。

[0064] 可选地，在接收移动终端发送的第一加密信息，基于所述第一加密信息和预存的第二加密信息进行身份验证之前，还包括：

[0065] 确定所述车机端中是否包括历史公钥；

[0066] 响应于包括所述历史公钥，确定所述历史公钥是否过期，如果过期，向云端请求更

新所述历史公钥;否则,将所述历史公钥作为所述第四公钥;

[0067] 响应于不包括所述历史公钥,向所述云端请求获取所述第四公钥并存储。

[0068] 可选地,所述向所述云端请求获取所述第四公钥并存储,包括:

[0069] 向所述云端发送信息请求;

[0070] 接收所述云端根据所述信息请求反馈的所述第四公钥;

[0071] 将所述第四公钥存入安全元件中。

[0072] 可选地,所述网络情况包括:网络正常情况和弱网络情况;

[0073] 所述根据网络情况,发起第二次钥匙验证,确定验证结果,包括:

[0074] 响应于所述网络情况为所述网络正常情况,通过云端实现所述车机端与所述移动终端的第二次钥匙验证;

[0075] 响应于所述网络情况为所述弱网络情况,通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证。

[0076] 可选地,所述通过云端实现所述车机端与所述移动终端的第二次钥匙验证,包括:

[0077] 将从所述移动终端接收的钥匙信息证书发送到所述云端;

[0078] 通过所述云端中存储的多个公钥中的一个公钥对所述钥匙信息证书进行解密得到钥匙信息;

[0079] 通过确认所述钥匙信息是否为使用过的钥匙信息,实现所述第二次钥匙验证。

[0080] 可选地,所述通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证,包括:

[0081] 向所述移动终端发送验证请求;

[0082] 接收通信服务端根据所述验证请求反馈的第二验证码和所述移动终端发送的第一验证码;

[0083] 比对所述第一验证码和所述第二验证码;

[0084] 响应于所述第一验证码和所述第二验证码相同,确定所述第二次钥匙验证通过。

[0085] 可选地,所述接收所述移动终端发送的第一验证码,包括:

[0086] 接收所述移动终端发送通过所述通信加密密钥进行加密得到加密验证码,通过所述通信加密密钥对所述加密验证码进行解密,得到所述第一验证码。

[0087] 可选地,还包括:

[0088] 响应于所述验证结果为通过验证,接收所述移动终端的控制;

[0089] 响应于所述验证结果为未通过验证,进入安全模式并发出提示信息。

[0090] 根据本申请实施例的又一方面,提供的一种移动终端,包括:

[0091] 身份验证模块,用于通过预存的第一加密信息,向车机端发起身份验证;其中,所述第一加密信息为车机身份数字证书经过第一私钥加密得到;

[0092] 第一钥匙验证模块,用于响应于所述身份验证通过,向所述车机端发起第一次钥匙验证;响应于所述第一次钥匙验证通过,所述车机端进入安全模式;

[0093] 第二钥匙验证模块,用于根据所述车机端的网络情况,接收所述车机端发起的第二次钥匙验证,确定验证结果。

[0094] 可选地,所述身份验证模块,具体用于将所述第一加密信息发送给所述车机端,通过所述车机端根据所述第一加密信息对所述移动终端的身份进行验证;接收所述车机端反

馈预存在所述车机端的第二加密信息;其中,所述第二加密信息为终端数字身份证书经过第二私钥加密得到;通过预存的第二公钥对所述第二加密信息进行解密,根据得到的终端数字身份证书确认所述车机端的身份。

[0095] 可选地,所述身份验证模块,还用于对接收的所述第二加密信息进行解密,获得所述车机端确认的通信加密方法和通信加密密钥;以所述通信加密方法和所述通信加密密钥加密后续与所述车机端之间的通信信息。

[0096] 可选地,所述第一钥匙验证模块,具体用于响应于所述身份验证通过,基于上一次钥匙验证使用的第三历史加密信息对应的历史序列号确定当前序列号;基于所述当前序列号确定本次通信的第三加密信息;其中,所述第三加密信息为钥匙信息证书经过第三公钥加密得到;将所述第三加密信息发送到所述车机端,所述车机端对所述第三加密信息进行验证,实现第一次钥匙验证。

[0097] 可选地,还包括:

[0098] 加密信息获取模块,用于确定所述移动终端中是否包括历史加密信息;响应于包括所述历史加密信息,确定所述历史加密信息是否过期,如果过期,向云端请求更新所述历史加密信息;否则,将所述历史加密信息作为所述第三加密信息;响应于不包括所述历史加密信息,向所述云端请求获取所述第三加密信息并存储。

[0099] 可选地,所述加密信息获取模块向所述云端请求获取所述第三加密信息并存储时,用于向所述云端发送信息请求;接收所述云端根据所述信息请求反馈的所述第三加密信息;将所述第三加密信息存入安全元件中。

[0100] 可选地,所述车机端的网络情况包括:网络正常情况和弱网络情况;

[0101] 所述第二钥匙验证模块,具体用于响应于所述车机端的网络情况为所述网络正常情况,通过云端实现所述车机端与所述移动终端的第二次钥匙验证;响应于所述车机端的网络情况为所述弱网络情况,通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证。

[0102] 可选地,所述第二钥匙验证模块在通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证时,用于向通信服务端发送所述车机端反馈的验证请求,接收所述通信服务端根据所述验证请求反馈的第一验证码;将所述第一验证码发送到所述车机端,通过所述车机端实现所述第二次钥匙验证。

[0103] 可选地,所述第二钥匙验证模块在将所述第一验证码发送到所述车机端时,用于将所述第一验证码通过所述通信加密密钥进行加密得到加密验证码;将所述加密验证码发送到所述车机端。

[0104] 可选地,还包括:

[0105] 验证结果模块,用于响应于所述验证结果为通过验证,控制所述车机端;响应于所述验证结果为未通过验证,所述车机端进入安全模式,所述车机端发出提示信息。

[0106] 根据本申请实施例的还一方面,提供的一种车机端,包括:

[0107] 身份验证模块,用于接收移动终端发送的第一加密信息,基于所述第一加密信息和预存的第二加密信息进行身份验证;其中,所述第一加密信息为车机身份数字证书经过第一私钥加密得到,所述第二加密信息为所述终端数字身份证书经过第二私钥加密得到;

[0108] 第一钥匙验证模块,用于响应于所述身份验证通过,接收所述移动终端发起的第

一次钥匙验证;响应于所述第一次钥匙验证通过,进入安全模式;

[0109] 第二钥匙验证模块,用于根据网络情况,发起第二次钥匙验证,确定验证结果。

[0110] 可选地,所述身份验证模块,具体用于接收所述移动终端发送的所述第一加密信息,根据预存的第一公钥对所述第一加密信息进行解密,根据解密得到车机身份数字证书确认所述移动终端的身份;响应于所述移动终端的身份合法,向所述移动终端发送第二加密信息到所述移动终端,所述移动终端根据所述第二加密信息对所述车机端的身份进行验证。

[0111] 可选地,所述身份验证模块,还用于对所述第一加密信息进行解密,获得所述移动终端确认的通信加密方法和通信加密密钥;以所述通信加密方法和所述通信加密密钥加密后续与所述移动终端之间的通信信息。

[0112] 可选地,所述第一钥匙验证模块,具体用于接收所述移动终端发送的第三加密信息并利用预存的第三私钥进行解密,得到钥匙信息证书;其中,所述第三加密信息为钥匙信息证书经过第三公钥加密得到;对所述钥匙信息证书进行验证,实现第一次钥匙验证。

[0113] 可选地,所述钥匙信息证书中包括:通过所述第三公钥加密的第一钥匙有效时间、通过所述第三公钥加密的私钥索引信息、以及通过第四私钥加密的第二钥匙有效时间和钥匙信息;其中,每个所述私钥索引信息对应一个第四公钥;

[0114] 所述第一钥匙验证模块在对所述钥匙信息证书进行验证,实现第一次钥匙验证时,用于通过所述第三公钥解密获得所述钥匙信息证书中的所述第一钥匙有效时间和所述私钥索引信息;通过所述私钥索引信息查找获得所述第四公钥;通过第四公钥对所述钥匙信息证书进一步解密,获得所述第二钥匙有效时间和所述钥匙信息;基于所述第一钥匙有效时间和所述第二钥匙有效时间对所述钥匙信息进行验证。

[0115] 可选地,所述第一钥匙验证模块在基于所述第一钥匙有效时间和所述第二钥匙有效时间对所述钥匙信息进行验证时,用于比对所述第一钥匙有效时间与所述第二钥匙有效时间;响应于所述第一钥匙有效时间与所述第二钥匙有效时间相等,根据所述第二钥匙有效时间和当前时间,确认所述钥匙信息是否在有效时间内;响应于所述钥匙信息在有效时间内确认验证通过。

[0116] 可选地,还包括:

[0117] 公钥获取模块,用于确定所述车机端中是否包括历史公钥;响应于包括所述历史公钥,确定所述历史公钥是否过期,如果过期,向云端请求更新所述历史公钥;否则,将所述历史公钥作为所述第四公钥;响应于不包括所述历史公钥,向所述云端请求获取所述第四公钥并存储。

[0118] 可选地,所述公钥获取模块在向所述云端请求获取所述第四公钥并存储时,用于向所述云端发送信息请求;接收所述云端根据所述信息请求反馈的所述第四公钥;将所述第四公钥存入安全元件中。

[0119] 可选地,所述网络情况包括:网络正常情况和弱网络情况;

[0120] 所述第二钥匙验证模块,具体用于响应于所述网络情况为所述网络正常情况,通过云端实现所述车机端与所述移动终端的第二次钥匙验证;响应于所述网络情况为所述弱网络情况,通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证。

[0121] 可选地,所述第二钥匙验证模块在通过云端实现所述车机端与所述移动终端的第

二次钥匙验证时，用于将从所述移动终端接收的钥匙信息证书发送到所述云端；通过所述云端中存储的多个公钥中的一个公钥对所述钥匙信息证书进行解密得到钥匙信息；通过确认所述钥匙信息是否为使用过的钥匙信息，实现所述第二次钥匙验证。

[0122] 可选地，所述第二钥匙验证模块在通过短信验证的方式实现所述车机端与所述移动终端的第二次钥匙验证时，用于向所述移动终端发送验证请求；接收通信服务端根据所述验证请求反馈的第二验证码和所述移动终端发送的第一验证码；比对所述第一验证码和所述第二验证码；响应于所述第一验证码和所述第二验证码相同，确定所述第二次钥匙验证通过。

[0123] 可选地，所述第二钥匙验证模块在接收所述移动终端发送的第一验证码时，具体用于接收所述移动终端发送通过所述通信加密密钥进行加密得到加密验证码，通过所述通信加密密钥对所述加密验证码进行解密，得到所述第一验证码。

[0124] 可选地，还包括：

[0125] 验证结果模块，用于响应于所述验证结果为通过验证，接收所述移动终端的控制；响应于所述验证结果为未通过验证，进入安全模式并发出提示信息。

[0126] 根据本申请实施例的再一方面，提供的一种通信验证系统，包括：

[0127] 如上述任意一项实施例所述的移动终端和如上述任意一项实施例所述的车机端。

[0128] 可选地，还包括：

[0129] 云端，用于向所述移动终端发送经过第一私钥加密的第一加密信息、经过第三公钥加密的第三加密信息和第二公钥，向所述车机端发送第二私钥加密的第二加密信息、第三私钥和第四公钥；并用于接收所述车机端发送的钥匙信息证书，基于存储的多个公钥中的一个供应对所述钥匙信息证书进行解密得到钥匙信息，确认所述钥匙信息是否为使用过的钥匙信息。

[0130] 基于本申请上述实施例提供的一种身份验证方法和系统、移动终端、车机端，通过预存的第一加密信息，向车机端发起身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到；响应于所述身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，所述车机端进入安全模式；根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果，本实施例通过身份验证以及两次钥匙验证提高了车机端的安全性，防止由于身份信息泄露或数据在传输过程中被截取篡改。

[0131] 下面通过附图和实施例，对本申请的技术方案做进一步的详细描述。

附图说明

[0132] 构成说明书的一部分的附图描述了本申请的实施例，并且连同描述一起用于解释本申请的原理。

[0133] 参照附图，根据下面的详细描述，可以更加清楚地理解本申请，其中：

[0134] 图1为本申请实施例提供的通信验证方法的一个流程示意图。

[0135] 图2是本公开图1所示的实施例中步骤102的一个流程示意图。

[0136] 图3是本公开图1所示的实施例中步骤104的一个流程示意图。

[0137] 图4为本申请实施例提供的通信验证方法的另一流程示意图。

[0138] 图5是本公开图4所示的实施例中步骤402的一个流程示意图。

[0139] 图6是本公开图4所示的实施例中步骤404的一个流程示意图。

[0140] 图7为本申请实施例提供的移动终端的一个结构示意图。

[0141] 图8为本申请实施例提供的车机端的一个结构示意图。

[0142] 图9为本申请实施例提供的通信验证系统中移动终端与车机端的一个时序示意图。

具体实施方式

[0143] 现在将参照附图来详细描述本申请的各种示例性实施例。应注意到:除非另外具体说明,否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本申请的范围。

[0144] 同时,应当明白,为了便于描述,附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0145] 以下对至少一个示例性实施例的描述实际上仅仅是说明性的,决不作为对本申请及其应用或使用的任何限制。

[0146] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论,但在适当情况下,所述技术、方法和设备应当被视为说明书的一部分。

[0147] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步讨论。

[0148] 图1为本申请实施例提供的通信验证方法的一个流程示意图。如图1所示,该方法应用于移动终端,该实施例方法包括:

[0149] 步骤102,通过预存的第一加密信息,向车机端发起身份验证。

[0150] 其中,第一加密信息为车机身份数字证书经过第一私钥加密得到。

[0151] 可选地,本实施例中的第一加密信息可以通过云端以第一私钥对车机身份数字证书进行加密后发送给移动终端获得,由于第一加密信息通过私钥加密,因此,车机端接收后需要使用对应该第一私钥的公钥进行解密,即,本实施例在身份验证时,采用的是非对称加密的方式实现,保证了车机身份数字证书的安全性。

[0152] 步骤104,响应于身份验证通过,向车机端发起第一次钥匙验证。

[0153] 可选地,本实施例还可以包括响应于身份验证不通过,结束本次身份验证。本实施例为了提高车机端的安全性,在身份验证通过后并不直接控制车机端与移动终端进行通信,而是进行第一次的钥匙验证,钥匙验证过程中通过车机端对移动终端中的钥匙信息进行验证,以确定该移动终端所持有的钥匙信息是否有效。

[0154] 步骤106,响应于第一次钥匙验证通过,车机端进入安全模式。

[0155] 可选地,本实施例还可以包括响应于第一次钥匙验证不通过,车机端拒绝移动终端的所有请求,结束本次通信验证。本实施例说明只有当移动终端中的钥匙信息是有效时,使车机端进入安全模式以进行第二次钥匙验证,进一步提高双方通信的安全性。

[0156] 可选地,本实施例中的安全模式可以是车机端的部分功能有所限制的模式,例如,车机端在安全模式下可以打开车门,但不能执行其他控制。

[0157] 步骤108,根据车机端的网络情况,接收车机端发起的第二次钥匙验证,确定验证

结果。

[0158] 现有技术中，在移动终端与车机端通信时，对于网络情况有要求，当网络情况较弱时，将无法实现通信。而本申请实施例为了解决在弱网络情况下，移动终端与车机端的安全通信，在进行第二次钥匙验证之前，需要对车机端的网络情况进行判断，根据判断结果(网络情况是强网络情况还是弱网络情况)，分别进行第二次钥匙验证，以保证在不同网络情况下移动终端与车机端都可以安全通信，不受网络情况限制。

[0159] 本申请上述实施例提供的一种身份验证方法，通过预存的第一加密信息，向车机端发起身份验证；其中，所述第一加密信息为车机身份数字证书经过第一私钥加密得到；响应于所述身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，所述车机端进入安全模式；根据所述车机端的网络情况，接收所述车机端发起的第二次钥匙验证，确定验证结果，本实施例通过身份验证以及两次钥匙验证，验证了通信双方的身份合法，避免任何一端通信密钥以及通信协议等相关信息泄漏，避免了攻击者恶意控制车辆进而引发安全事故。

[0160] 如图2所示，在上述图1所示实施例的基础上，步骤102可包括如下步骤：

[0161] 步骤1021，将第一加密信息发送给车机端，通过车机端根据第一加密信息对移动终端的身份进行验证。

[0162] 由于第一加密信息中被加密的是车机身份数字证书，因此，需发送到对应的车机端进行认证，以确认该车机身份数字证书与车机端之间的对应关系。

[0163] 步骤1022，接收车机端反馈预存在车机端的第二加密信息。

[0164] 其中，第二加密信息为终端数字身份证书经过第二私钥加密得到。

[0165] 本实施例中，车机端存储有第二加密信息，可选地，该第二加密信息可以通过云端以第二私钥加密终端数字身份证书获得，并且，云端在加密之后将该第二加密信息发送给车机端保存，车机端存储该终端数字身份证书，说明该终端数字身份证书对应的移动终端与该车机端相对应。

[0166] 步骤1023，通过预存的第二公钥对第二加密信息进行解密，根据得到的终端数字身份证书确认车机端的身份。

[0167] 本实施例中通过加密处理的第二私钥对应的第二公钥对第二加密信息进行解密，实现非对称解密，根据解密得到的终端数字身份证书与移动终端中的身份信息进行匹配，当终端数字身份证书与移动终端中的身份信息相适配时，说明发送该第二加密信息的车机端与移动终端相对应。

[0168] 可选地，步骤102在进行身份验证的同时，还包括：

[0169] 对接收的第二加密信息进行解密，获得车机端确认的通信加密方法和通信加密密钥；以通信加密方法和通信加密密钥加密后续与车机端之间的通信信息。

[0170] 可选地，移动终端与车机端的通信过程为了得到安全保证，必须使用的对称加密算法，但是协商对称加密算法的过程，需要使用非对称加密算法(本实施例中身份验证过程)来保证安全，然而直接使用非对称加密的过程本身也不安全，会有中间人篡改公钥的可能性，因此，本实施例中移动终端与车机端不直接使用公钥，而是使用第三方数字证书认证机构(certificate authority，CA)及其发送的公钥来保证非对称加密过程本身的安全，例如，云端分别使用第一私钥和第二私钥对车机身份数字证书和终端身份数字证书进行加

密，并将第一私钥对应的第一公钥发送给车机端，将第二私钥对应的第二公钥发送给移动终端。即通过非对称加密算法协商出一个对称加密算法，之后传输的所有数据，都通过通信密钥加密；这样网路上的其它用户，将很难窃取和篡改移动终端和车机端之间传输的数据，从而保证了数据的私密性和完整性，即保证了通信内容的安全。

[0171] 如图3所示，在上述图1所示实施例的基础上，步骤104可包括如下步骤：

[0172] 步骤1041，响应于身份验证通过，基于上一次钥匙验证使用的第三历史加密信息对应的历史序列号确定当前序列号。

[0173] 本实施例中，上一次解锁指上一次通过第一身份验证之后向车机端发送存储的钥匙信息证书请求开锁的过程；移动终端中存储有多个钥匙信息证书，其中，每个钥匙信息证书仅能应用一次，可有效防止钥匙被拦截导致其他非法开锁的行为发生；因此，在本次发送钥匙信息证书之前，先通过历史序列号确定当前序列号，例如，对历史序列号加一得到当前序列号。

[0174] 可选地，移动终端取出记录上次已使用钥匙信息证书的序列号(index)值加1，若没有记录过则从0开始，例如，当前index等于0，则读取预先存储安全元件(Secure Element，SE)中的多个钥匙信息证书中序列为1的证书，发送给车机端。

[0175] 步骤1042，基于当前序列号确定本次通信的第三加密信息。

[0176] 其中，第三加密信息为钥匙信息证书经过第三公钥加密得到。

[0177] 为了保证移动终端与车机端之间的发送钥匙信息的安全，本实施例通过非对称加密方法对钥匙信息证书进行传输。

[0178] 步骤1043，将第三加密信息发送到车机端，车机端对第三加密信息进行验证，实现第一次钥匙验证。

[0179] 本实施例中，车机端中存储有一个私钥(对应第三公钥)和多个钥匙信息相关公钥；云端存储有一个车机端私钥对应的公钥和多个钥匙信息相关私钥；移动终端存储由云端下发的多个钥匙信息证书，钥匙信息证书主要包括：通过第三公钥加密的第一钥匙有效时间、通过第三公钥加密的私钥索引信息、通过第四私钥加密的第二钥匙有效时间以及第四私钥加密的钥匙信息。

[0180] 在一些可选的实施例中，在执行步骤102之前，还包括：

[0181] 确定移动终端中是否包括历史加密信息。

[0182] 响应于包括历史加密信息，确定历史加密信息是否过期，如果过期，向云端请求更新历史加密信息；否则，将历史加密信息作为第三加密信息。

[0183] 响应于不包括历史加密信息，向云端请求获取第三加密信息。

[0184] 本实施例中，移动终端将获取的钥匙信息证书(本实施例中为钥匙信息证书经过加密后的第三加密信息)使用可信执行环境(Trusted Execution Environment，TEE)提供可信赖的运行环境，将对机密性、完整性的保护和数据访问权限的控制，来确保密钥存储的安全。

[0185] 可选地，向云端请求获取第三加密信息并存储，包括：

[0186] 向云端发送信息请求；

[0187] 接收云端根据信息请求反馈的第三加密信息；

[0188] 将第三加密信息存入安全元件中。

[0189] 本实施例中，当移动终端中不包括第三加密信息时，需向云端等第三方请求获取第三加密信息，并将获得的第三加密信息保存在安全元件中，可选地，安全元件包括但不限于：硬件TEE芯片、软件TEE环境以及SE安全元件，优先使用SE若没有，再检查是否可存储于硬件TEE，若也没有硬件TEE，再检查是否可存储于软件TEE，以确保了第三加密信息的安全存储。

[0190] 在一些可选的实施例中，车机端的网络情况包括：网络正常情况和弱网络情况；对应不同网络情况，步骤106可以包括：

[0191] 响应于车机端的网络情况为网络正常情况，通过云端实现车机端与移动终端的第二次钥匙验证。

[0192] 响应于车机端的网络情况为弱网络情况，通过短信验证的方式实现车机端与移动终端的第二次钥匙验证。

[0193] 本实施例中，第二次钥匙验证根据当前车机端所处的网络强弱分为两种：一种云端校验，若车机端所处的网络状态良好，同步移动智能终端发来的证书至服务器验证，若验证通过则解除安全模式，进入正常模式；若验证失败，则通知车主关注车辆情况；另外一种为第三方SP短信服务来完成校验，例如，处于2G网络可收发短信服务器状态，则进入5分钟计时。5分钟内，车机系统请求发送高级权限验证给移动智能终端，移动智能终端收到后，弹窗提示用户选择安全模式与正常模式，若选择安全模式，则发送请求通知车机系统直接计时结束，车辆进入安全模式；若选择正常模式，移动智能终端通过向SP服务发送短信，请求下发验证码，SP服务收到请求下发验证码短信后，短信通知移动智能终端以及车机端，车机端收到验证码后存储保存，移动智能端，将收到的验证码发送给车机端，车机端将移动智能端发来的验证码与自己收取后存储的验证码比较，若相同，则验证通过，车机端停止计时，车辆进入正常模式；若不相同，车机系统发送请求反馈智能终端提示验证码错误，请重新输入，此逻辑顺序一直循环，直到验证码验证通过。5分钟后，车机系统自动进入安全模式。

[0194] 若为无网络状态，则车辆自动进入安全模式；待车辆行驶到网络条件好的地段，车辆连上网后，同步移动智能终端发来的证书至服务器验证，若验证通过则解除安全模式，进入正常模式；若验证失败，则通知车主关注车辆情况。

[0195] 可选地，短信验证过程可以包括：

[0196] 向通信服务端发送车机端反馈的验证请求，接收通信服务端根据验证请求反馈的第一验证码；将第一验证码发送到车机端，通过车机端实现第二次钥匙验证。

[0197] 本实施例中，为了提高验证码在移动终端与车机端之间传输的安全性，可选地，将第一验证码通过通信加密密钥进行加密得到加密验证码；将加密验证码发送到车机端。即，通过身份验证时通过非对称加密协商得到的对称加密密码对第一验证码进行加密，传输加密后的加密验证码，增强了第一验证码的安全性。

[0198] 在一些可选的实施例中，本实施例提供的方法还包括：

[0199] 响应于验证结果为通过验证，控制车机端；

[0200] 响应于验证结果为未通过验证，车机端进入安全模式，车机端发出提示信息。

[0201] 本实施例中，移动终端通过两次钥匙验证之后，将获得对车机端的控制权，实现对车机端的控制，例如，开锁、开启空调等；实现对车辆的安全控制；而当验证结果表示未通过验证时，为保证车机端的安全，车机端进入安全模式，防止被无权限终端控制，提高了车辆

的安全性，同时，可向车主发出提示信息。

[0202] 图4为本申请实施例提供的通信验证方法的另一流程示意图。如图4所示，该方法应用于车机端，该实施例方法包括：

[0203] 步骤402，接收移动终端发送的第一加密信息，基于第一加密信息和预存的第二加密信息进行身份验证。

[0204] 其中，第一加密信息为车机身份数字证书经过第一私钥加密得到，第二加密信息为终端数字身份证书经过第二私钥加密得到。

[0205] 可选地，本实施例中车机端根据接收的第一加密信息对移动终端的身份进行验证，并发送第二加密信息给移动终端进行验证；其中，第二加密信息可以通过云端以第二私钥对终端数字身份证书进行加密后发送给车机端获得，由于第二加密信息通过私钥加密，因此，移动终端接收后需要使用对应第二私钥的公钥进行解密，即，本实施例在身份验证时，采用的是非对称加密的方式实现，保证了终端身份数字证书的安全性。

[0206] 步骤404，响应于身份验证通过，接收移动终端发起的第一次钥匙验证。

[0207] 可选地，本实施例还可以包括响应于身份验证不通过，结束本次身份验证。本实施例为了提高车机端的安全性，在身份验证通过后并不直接控制车机端与移动终端进行通信，而是进行第一次的钥匙验证，钥匙验证过程中通过车机端对移动终端中的钥匙信息进行验证，以确定该移动终端所持有的钥匙信息是否有效。

[0208] 步骤406，响应于第一次钥匙验证通过，进入安全模式。

[0209] 可选地，本实施例还可以包括响应于第一次钥匙验证不通过，车机端拒绝移动终端的所有请求，结束本次通信验证。本实施例说明只有当移动终端中的钥匙信息是有效时，使车机端进入安全模式以进行第二次钥匙验证，进一步提高双方通信的安全性。

[0210] 步骤408，根据网络情况，发起第二次钥匙验证，确定验证结果。

[0211] 本申请上述实施例提供的一种身份验证方法，接收移动终端发送的第一加密信息，基于第一加密信息和预存的第二加密信息进行身份验证；其中，第一加密信息为车机身份数字证书经过第一私钥加密得到，第二加密信息为终端数字身份证书经过第二私钥加密得到；响应于身份验证通过，接收所述移动终端发起的第一次钥匙验证；响应于所述第一次钥匙验证通过，进入安全模式；根据网络情况，发起第二次钥匙验证，确定验证结果，本实施例通过身份验证以及两次钥匙验证，验证了通信双方的身份合法，避免任何一端通信密钥以及通信协议等相关信息泄漏，避免了攻击者恶意控制车辆进而引发安全事故。

[0212] 如图5所示，在上述4所示实施例的基础上，步骤402可包括如下步骤：

[0213] 步骤4021，接收移动终端发送的第一加密信息，根据预存的第一公钥对第一加密信息进行解密，根据解密得到车机身份数字证书确认移动终端的身份。

[0214] 步骤4022，响应于移动终端的身份合法，向移动终端发送第二加密信息到移动终端，移动终端根据第二加密信息对车机端的身份进行验证。

[0215] 可选地，本实施例还可以包括响应于移动终端的身份不合法，停止身份验证，还可以发送信息提示车主出现非法访问等。

[0216] 本实施例中，通过在移动终端保存车机身份数字证书，在车机端保存终端身份数字证书的方式实现双向身份验证；车机端根据接收的车机身份数字证书与本地标识进行对比，即可确定发送车机身份数字证书的终端设备身份是否合法，只有当移动终端的身份合

法，车机端才发送第二加密信息给移动终端，移动终端根据第二加密信息验证车机端的身份。

[0217] 可选地，步骤402在进行身份验证的同时，还包括：

[0218] 对第一加密信息进行解密，获得移动终端确认的通信加密方法和通信加密密钥；以通信加密方法和通信加密密钥加密后续与移动终端之间的通信信息。

[0219] 本实施例中，为了使移动终端与车机端的通信过程得到安全保证，须使用的对称加密算法，本实施例为了提高协商对称加密算法过程的安全，使用了非对称加密算法来进行算法协商，在非对称加密过程使用的密钥安全由安全元件存储来解决。通过这些机制在身份认证的同时协商出一个对称加密算法及密钥，使双方后续通信安全得到解决。

[0220] 如图6所示，在上述4所示实施例的基础上，步骤404可包括如下步骤：

[0221] 步骤4041，接收移动终端发送的第三加密信息并利用预存的第三私钥进行解密，得到钥匙信息证书。

[0222] 其中，第三加密信息为钥匙信息证书经过第三公钥加密得到。

[0223] 步骤4042，对钥匙信息证书进行验证，实现第一次钥匙验证。

[0224] 本实施例中，车机端中存储有一个私钥(对应第三公钥)和多个钥匙信息相关公钥；云端存储有一个车机端私钥对应的公钥和多个钥匙信息相关私钥；移动终端存储由云端下发的多个钥匙信息证书，钥匙信息证书主要包括：通过第三公钥加密的第一钥匙有效时间、通过第三公钥加密的私钥索引信息、通过第四私钥加密的第二钥匙有效时间以及第四私钥加密的钥匙信息。

[0225] 可选地，钥匙信息证书中包括：通过第三公钥加密的第一钥匙有效时间、通过第三公钥加密的私钥索引信息、以及通过第四私钥加密的第二钥匙有效时间和钥匙信息；其中，每个私钥索引信息对应一个第四公钥；

[0226] 可选地，步骤4042包括：

[0227] 通过第三公钥解密获得钥匙信息证书中的第一钥匙有效时间和私钥索引信息；

[0228] 通过私钥索引信息查找获得第四公钥；

[0229] 通过第四公钥对钥匙信息证书进一步解密，获得第二钥匙有效时间和钥匙信息；

[0230] 基于第一钥匙有效时间和第二钥匙有效时间对钥匙信息进行验证。

[0231] 基于安全通信，车机端接受钥匙信息后，用对应第三公钥的第三私钥对第三加密信息进行解密，解密后获得钥匙信息证书中的第一有效时间以及私钥索引(index)信息；根据index找到对应的第四公钥，再用第四公钥解密钥匙信息证书，得到第二钥匙有效时间和钥匙信息，通过比较第一钥匙有效时间和第二钥匙有效时间是否一致确定该钥匙信息是否有效，当第一钥匙有效时间和第二钥匙有效时间是一致，且钥匙信息未超出第一钥匙有效时间(或第二钥匙有效时间)时，完成钥匙信息的认证，得到有效的钥匙信息。

[0232] 可选地，基于第一钥匙有效时间和第二钥匙有效时间对钥匙信息进行验证，包括：

[0233] 比对第一钥匙有效时间与第二钥匙有效时间；

[0234] 响应于第一钥匙有效时间与第二钥匙有效时间相等，根据第二钥匙有效时间和当前时间，确认钥匙信息是否在有效时间内；

[0235] 响应于钥匙信息在有效时间内确认验证通过。

[0236] 在一些可选的实施例中，在执行步骤402之前，还包括：

[0237] 确定车机端中是否包括历史公钥。

[0238] 响应于包括历史公钥，确定历史公钥是否过期，如果过期，向云端请求更新历史公钥；否则，将历史公钥作为第四公钥；

[0239] 响应于不包括历史公钥，向云端请求获取第四公钥并存储。

[0240] 本实施例中，在车机端与移动智能终端在网络正常时，移动智能终端预先请求获取云端获取多个钥匙信息证书(经加密为第三加密信息)，并存储于安全环境中；车机端预先通过SCP03协议预先获取多个钥匙信息证书对应公钥(第三加密信息对应的第四公钥)存储于安全环境中，安全存储有硬件TEE芯片、软件TEE环境以及SE安全元件，优先使用SE若没有，再检查是否可存储于硬件TEE，若也没有硬件TEE，再检查是否可存储于软件TEE，来确保了数字证书的安全存储问题。其中，在SE安全元件中具有加密/解密逻辑电路，车机端通过SCP03协议获取云端密钥证书并将密钥存储于SE安全元件中可保证密钥存储安全。可选地，向云端请求获取第四公钥并存储，包括：

[0241] 向云端发送信息请求；

[0242] 接收云端根据信息请求反馈的第四公钥；

[0243] 将第四公钥存入安全元件中。

[0244] 在一些可选的实施例中，车机端的网络情况包括：网络正常情况和弱网络情况；对应不同网络情况，步骤406可以包括：

[0245] 响应于网络情况为网络正常情况，通过云端实现车机端与移动终端的第二次钥匙验证；

[0246] 响应于网络情况为弱网络情况，通过短信验证的方式实现车机端与移动终端的第二次钥匙验证。

[0247] 本实施例中，第二次钥匙验证根据当前车机端所处的网络强弱分为两种：一种云端校验，若车机端所处的网络状态良好，同步移动智能终端发来的证书至服务器验证，若验证通过则解除安全模式，进入正常模式；若验证失败，则通知车主关注车辆情况；另外一种为第三方SP短信服务来完成校验。

[0248] 可选地，通过云端实现第二次钥匙验证，包括：

[0249] 将从移动终端接收的钥匙信息证书发送到云端；

[0250] 通过云端中存储的多个公钥中的一个公钥对钥匙信息证书进行解密得到钥匙信息；

[0251] 通过确认钥匙信息是否为使用过的钥匙信息，实现第二次钥匙验证。

[0252] 本实施例中，当车机端的网络情况为网络正常情况时，由车机端发起第二次钥匙验证，此时，车机端将接收的钥匙信息证书发送到云端进行验证，避免了本地验证可能被篡改的可能性，提高了钥匙证书验证的安全性和可靠性。

[0253] 可选地，通过短信验证的方式实现第二次钥匙验证，包括：

[0254] 向移动终端发送验证请求；

[0255] 接收通信服务端根据验证请求反馈的第二验证码和移动终端发送的第一验证码；

[0256] 比对第一验证码和第二验证码；

[0257] 响应于第一验证码和第二验证码相同，确定第二次钥匙验证通过。

[0258] 本实施例中，通过通信服务端(例如，SP服务等)发送的验证码实现两端的第二次

钥匙验证，该验证码的获取由移动终端向通信服务端请求，通信服务端向移动终端和车机端分别反馈内容相同的第一验证码和第二验证码；车机端通过比对从移动终端接收的第一验证码与从通信服务端接收的第二验证码是否相同，当第一验证码和第二验证码相同，确定本次身份验证通过。

[0259] 可选地，接收移动终端发送的第一验证码，包括：接收移动终端发送通过通信加密密钥进行加密得到加密验证码，通过通信加密密钥对加密验证码进行解密，得到第一验证码。

[0260] 本实施例中，为了提高验证码在移动终端与车机端之间传输的安全性，可选地，将第一验证码通过通信加密密钥进行加密得到加密验证码；将加密验证码发送到车机端。即，通过身份验证时通过非对称加密协商得到的对称加密密码对第一验证码进行加密，传输加密后的加密验证码，增强了第一验证码的安全性。

[0261] 在一些可选的实施例中，本实施例提供的方法还包括：

[0262] 响应于验证结果为通过验证，接收移动终端的控制；

[0263] 响应于验证结果为未通过验证，进入安全模式并发出提示信息。

[0264] 本实施例中，移动终端通过两次钥匙验证之后，将获得对车机端的控制权，实现对车机端的控制，例如，开锁、开启空调等；实现对车辆的安全控制；而当验证结果表示未通过验证时，为保证车机端的安全，车机端进入安全模式，防止被无权限终端控制，提高了车辆的安全性，同时，可向车主发出提示信息。

[0265] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0266] 图7为本申请实施例提供的移动终端的一个结构示意图。该实施例的移动终端可用于实现本申请上述各方法实施例。如图7所示，该实施例的移动终端包括：

[0267] 身份验证模块71，用于通过预存的第一加密信息，向车机端发起身份验证。

[0268] 其中，第一加密信息为车机身份数字证书经过第一私钥加密得到。

[0269] 第一钥匙验证模块72，用于响应于身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，车机端进入安全模式。

[0270] 第二钥匙验证模块73，用于根据车机端的网络情况，接收车机端发起的第二次钥匙验证，确定验证结果。

[0271] 本申请上述实施例提供的移动终端，通过预存的第一加密信息，向车机端发起身份验证；其中，第一加密信息为车机身份数字证书经过第一私钥加密得到；响应于身份验证通过，向所述车机端发起第一次钥匙验证；响应于所述第一次钥匙验证通过，车机端进入安全模式；根据车机端的网络情况，接收车机端发起的第二次钥匙验证，确定验证结果，本实施例通过身份验证以及两次钥匙验证，验证了通信双方的身份合法，避免任何一端通信密钥以及通信协议等相关信息泄漏，避免了攻击者恶意控制车辆进而引发安全事故。

[0272] 在一些可选的实施例中，身份验证模块71，具体用于将第一加密信息发送给车机端，通过车机端根据第一加密信息对移动终端的身份进行验证；接收车机端反馈预存在车机端的第二加密信息；其中，第二加密信息为终端数字身份证书经过第二私钥加密得到；通

过预存的第二公钥对第二加密信息进行解密，根据得到的终端数字身份证书确认车机端的身份。

[0273] 可选地，身份验证模块71，还用于对接收的第二加密信息进行解密，获得车机端确认的通信加密方法和通信加密密钥；以通信加密方法和通信加密密钥加密后续与车机端之间的通信信息。

[0274] 可选地，第一钥匙验证模块72，具体用于响应于身份验证通过，基于上一次钥匙验证使用的第三历史加密信息对应的历史序列号确定当前序列号；基于当前序列号确定本次通信的第三加密信息；其中，第三加密信息为钥匙信息证书经过第三公钥加密得到；将第三加密信息发送到车机端，车机端对第三加密信息进行验证，实现第一次钥匙验证。

[0275] 可选地，本实施例提供的移动终端还包括：

[0276] 加密信息获取模块，用于确定移动终端中是否包括历史加密信息；响应于包括历史加密信息，确定历史加密信息是否过期，如果过期，向云端请求更新历史加密信息；否则，将历史加密信息作为第三加密信息；响应于不包括历史加密信息，向云端请求获取第三加密信息并存储。

[0277] 可选地，加密信息获取模块向云端请求获取第三加密信息并存储时，用于向云端发送信息请求；接收云端根据信息请求反馈的第三加密信息；将第三加密信息存入安全元件中。

[0278] 在一些可选的实施例中，车机端的网络情况包括：网络正常情况和弱网络情况；

[0279] 第二钥匙验证模块73，具体用于响应于车机端的网络情况为网络正常情况，通过云端实现车机端与移动终端的第二次钥匙验证；响应于车机端的网络情况为弱网络情况，通过短信验证的方式实现车机端与移动终端的第二次钥匙验证。

[0280] 可选地，第二钥匙验证模块73在通过短信验证的方式实现车机端与移动终端的第二次钥匙验证时，用于向通信服务端发送车机端反馈的验证请求，接收通信服务端根据验证请求反馈的第一验证码；将第一验证码发送到车机端，通过车机端实现第二次钥匙验证。

[0281] 可选地，第二钥匙验证模块73在将第一验证码发送到车机端时，用于将第一验证码通过通信加密密钥进行加密得到加密验证码；将加密验证码发送到车机端。

[0282] 在一些可选的实施例中，本实施例提供的移动终端还包括：

[0283] 验证结果模块，用于响应于验证结果为通过验证，控制车机端；响应于验证结果为未通过验证，车机端进入安全模式，车机端发出提示信息。

[0284] 图8为本申请实施例提供的车机端的一个结构示意图。该实施例的移动终端可用于实现本申请上述各方法实施例。如图8所示，该实施例的车机端包括：

[0285] 身份验证模块81，用于接收移动终端发送的第一加密信息，基于第一加密信息和预存的第二加密信息进行身份验证。

[0286] 其中，第一加密信息为车机身份数字证书经过第一私钥加密得到，第二加密信息为终端数字身份证书经过第二私钥加密得到。

[0287] 第一钥匙验证模块82，用于响应于身份验证通过，接收移动终端发起的第一次钥匙验证；响应于第一次钥匙验证通过，进入安全模式。

[0288] 第二钥匙验证模块83，用于根据网络情况，发起第二次钥匙验证，确定验证结果。

[0289] 本申请上述实施例提供的车机端，接收移动终端发送的第一加密信息，基于第一

加密信息和预存的第二加密信息进行身份验证;其中,第一加密信息为车机身份数字证书经过第一私钥加密得到,第二加密信息为终端数字身份证书经过第二私钥加密得到;响应于身份验证通过,接收移动终端发起的第一次钥匙验证;响应于第一次钥匙验证通过,进入安全模式;根据网络情况,发起第二次钥匙验证,确定验证结果,本实施例通过身份验证以及两次钥匙验证,验证了通信双方的身份合法,避免任何一端通信密钥以及通信协议等相关信息泄漏,避免了攻击者恶意控制车辆进而引发安全事故。

[0290] 在一些可选的实施例中,身份验证模块81,具体用于接收移动终端发送的第一加密信息,根据预存的第一公钥对第一加密信息进行解密,根据解密得到车机身份数字证书确认移动终端的身份;响应于移动终端的身份合法,向移动终端发送第二加密信息到移动终端,移动终端根据第二加密信息对车机端的身份进行验证。

[0291] 可选地,身份验证模块81,还用于对第一加密信息进行解密,获得移动终端确认的通信加密方法和通信加密密钥;以通信加密方法和通信加密密钥加密后续与移动终端之间的通信信息。

[0292] 在一些可选的实施例中,第一钥匙验证模块82,具体用于接收移动终端发送的第三加密信息并利用预存的第三私钥进行解密,得到钥匙信息证书;其中,第三加密信息为钥匙信息证书经过第三公钥加密得到;对钥匙信息证书进行验证,实现第一次钥匙验证。

[0293] 可选地,钥匙信息证书中包括:通过第三公钥加密的第一钥匙有效时间、通过第三公钥加密的私钥索引信息、以及通过第四私钥加密的第二钥匙有效时间和钥匙信息;其中,每个私钥索引信息对应一个第四公钥;

[0294] 第一钥匙验证模块82在对钥匙信息证书进行验证,实现第一次钥匙验证时,用于通过第三公钥解密获得钥匙信息证书中的第一钥匙有效时间和私钥索引信息;通过私钥索引信息查找获得第四公钥;通过第四公钥对钥匙信息证书进一步解密,获得第二钥匙有效时间和钥匙信息;基于第一钥匙有效时间和第二钥匙有效时间对钥匙信息进行验证。

[0295] 可选地,第一钥匙验证模块82在基于第一钥匙有效时间和第二钥匙有效时间对钥匙信息进行验证时,用于比对第一钥匙有效时间与第二钥匙有效时间;响应于第一钥匙有效时间与第二钥匙有效时间相等,根据第二钥匙有效时间和当前时间,确认钥匙信息是否在有效时间内;响应于钥匙信息在有效时间内确认验证通过。

[0296] 可选地,本实施例提供的车机端还包括:

[0297] 公钥获取模块,用于确定车机端中是否包括历史公钥;响应于包括历史公钥,确定历史公钥是否过期,如果过期,向云端请求更新历史公钥;否则,将历史公钥作为第四公钥;响应于不包括历史公钥,向云端请求获取第四公钥并存储。

[0298] 可选地,公钥获取模块在向云端请求获取第四公钥并存储时,用于向云端发送信息请求;接收云端根据信息请求反馈的第四公钥;将第四公钥存入安全元件中。

[0299] 在一些可选的实施例中,网络情况包括:网络正常情况和弱网络情况;

[0300] 第二钥匙验证模块83,具体用于响应于网络情况为网络正常情况,通过云端实现车机端与移动终端的第二次钥匙验证;响应于网络情况为弱网络情况,通过短信验证的方式实现车机端与移动终端的第二次钥匙验证。

[0301] 可选地,第二钥匙验证模块83在通过云端实现车机端与移动终端的第二次钥匙验证时,用于将从移动终端接收的钥匙信息证书发送到云端;通过云端中存储的多个公钥中

的一个公钥对钥匙信息证书进行解密得到钥匙信息;通过确认钥匙信息是否为使用过的钥匙信息,实现第二次钥匙验证。

[0302] 可选地,第二钥匙验证模块83在通过短信验证的方式实现车机端与移动终端的第二次钥匙验证时,用于向移动终端发送验证请求;接收通信服务端根据验证请求反馈的第二验证码和移动终端发送的第一验证码;比对第一验证码和第二验证码;响应于第一验证码和第二验证码相同,确定第二次钥匙验证通过。

[0303] 可选地,第二钥匙验证模块83在接收移动终端发送的第一验证码时,具体用于接收移动终端发送通过通信加密密钥进行加密得到加密验证码,通过通信加密密钥对加密验证码进行解密,得到第一验证码。

[0304] 可选地,还包括:

[0305] 验证结果模块,用于响应于验证结果为通过验证,接收移动终端的控制;响应于验证结果为未通过验证,进入安全模式并发出提示信息。

[0306] 根据本申请实施例的另一方面,提供的一种通信验证系统,包括:

[0307] 如上述任意一项实施例提供的移动终端和如上述任意一项实施例提供的车机端。

[0308] 图9为本申请实施例提供的通信验证系统中移动终端(移动智能终端)与车机端的一个时序示意图。如图9所示,当车机端或移动智能终端处于弱网络环境下,通过蓝牙通信。

[0309] 移动智能终端读取预先内置于TEE环境中的标识车机身份数字证书,发送至车机端。车机端验证证书,确认移动智能终端身份合法;车机端读取预先内置移动端身份的数字证书,发送至移动智能终端,移动智能终端验证证书,确认车机端身份合法,并在此过程协商通信加密算法,确定通信加密算法,至此,通信环境基本保证安全。

[0310] 移动智能终端取出记录上次已使用钥匙信息证书的序列号index值加1,若没有记录过则从0开始,例如,当前index等于0,则读取预先存储SE安全元件中的多个钥匙信息证书中序列为1的证书,发送给车机端,车机端接受钥匙信息证书并用私钥解密钥匙中公钥加密信息,获得钥匙信息中有效时间以及公钥index索引信息以及确定钥匙信息证书合法;确认index索引等于lastIndex(上次验证通过的index索引值加1),否则钥匙信息认证失败,若index索引验证通过再验证lastIndex已上报云端,若没有则发短信通知车主关注车辆是否安全。再根据index索引找到对应公钥,解密获得私钥加密的钥匙有效时间,比对钥匙信息一致以及确认钥匙在有效期内,完成钥匙信息认证。

[0311] 此时,车辆(车机端)进入安全模式,为了更好保证车辆安全,需要二次确认钥匙信息。二次确认执行方案依据当前车辆网络强弱分为两种:一种云端校验,另外一种为第三方SP短信服务来完成。

[0312] 若车辆网络状态良好,同步移动智能终端发来的证书至云端验证,若验证通过则解除安全模式,进入正常模式;若验证失败,则通知车主关注车辆情况。

[0313] 若为无网络状态,则车辆自动进入安全模式;待车辆行驶到网络条件好的地段,车辆连上网后,同步移动智能终端发来的证书至服务器验证,若验证通过则解除安全模式,进入正常模式;若验证失败,则通知车主关注车辆情况。

[0314] 若处于2G网络可收发短信服务器状态,则进入5分钟计时。5分钟内,车机系统请求发送高级权限验证给移动智能终端,移动智能终端收到后,弹窗提示用户选择安全模式与正常模式,若选择安全模式,则发送请求通知车机系统直接计时结束,车辆进入安全模式;

若选择正常模式，移动智能终端通过向SP服务发送短信，请求下发验证码，SP服务收到请求下发验证码短信后，短信通知移动智能终端以及车机端，车机端收到验证码后存储保存，移动智能端，将收到的验证码发送给车机端，车机端将移动智能端发来的验证码与自己收取后存储的验证码比较，若相同，则验证通过，车机端停止计时，车辆进入正常模式；若不相同，车机系统发送请求反馈智能终端提示验证码错误，请重新输入，此逻辑顺序一直循环，直到验证码验证通过。5分钟后，车机系统自动进入安全模式。

[0315] 可选地，通信验证系统还可以包括：

[0316] 云端，用于向移动终端发送经过第一私钥加密的第一加密信息、经过第三公钥加密的第三加密信息和第二公钥，向车机端发送第二私钥加密的第二加密信息、第三私钥和第四公钥；并用于接收车机端发送的钥匙信息证书，基于存储的多个公钥中的一个供应对钥匙信息证书进行解密得到钥匙信息，确认钥匙信息是否为使用过的钥匙信息。

[0317] 可能以许多方式来实现本申请的方法和装置。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本申请的方法和装置。用于所述方法的步骤的上述顺序仅是为了进行说明，本申请的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本申请实施为记录在记录介质中的程序，这些程序包括用于实现根据本申请的方法的机器可读指令。因而，本申请还覆盖存储用于执行根据本申请的方法的程序的记录介质。

[0318] 本申请的描述是为了示例和描述起见而给出的，而并不是无遗漏的或者将本申请限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描述实施例是为了更好说明本申请的原理和实际应用，并且使本领域的普通技术人员能够理解本申请从而设计适于特定用途的带有各种修改的各种实施例。

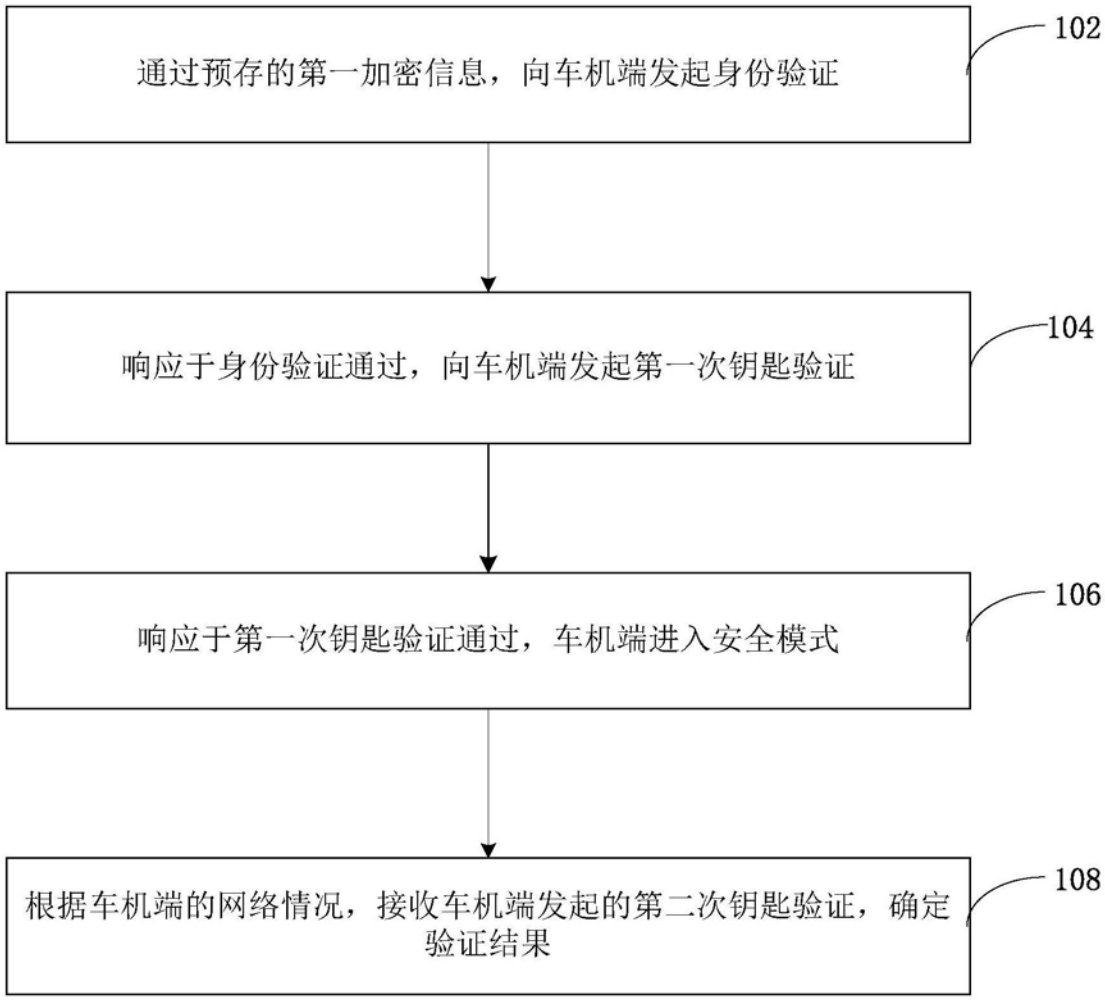

通过预存的第一加密信息，向车机端发起身份验证
102
响应于身份验证通过，向车机端发起第一次钥匙验证
104
响应于第一次钥匙验证通过，车机端进入安全模式
106
根据车机端的网络情况，接收车机端发起的第二次钥匙验证，确定验证结果
108

图1

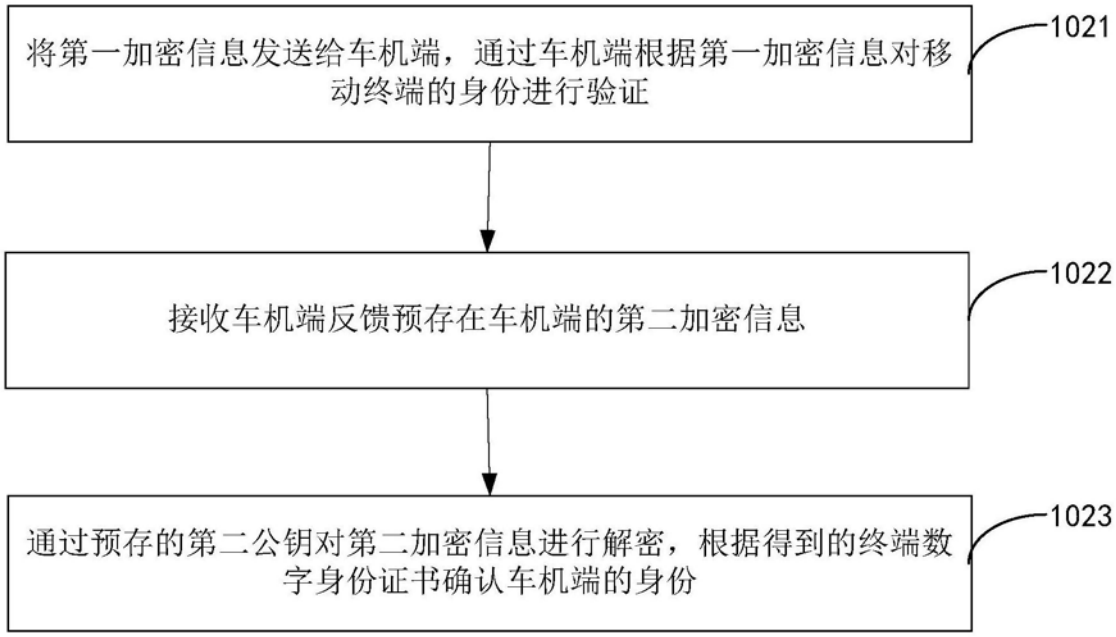

将第一加密信息发送给车机端，通过车机端根据第一加密信息对移动终端的身份进行验证
1021
接收车机端反馈预存在车机端的第二加密信息
1022
通过预存的第二公钥对第二加密信息进行解密，根据得到的终端数字身份证书确认车机端的身份
1023

图2

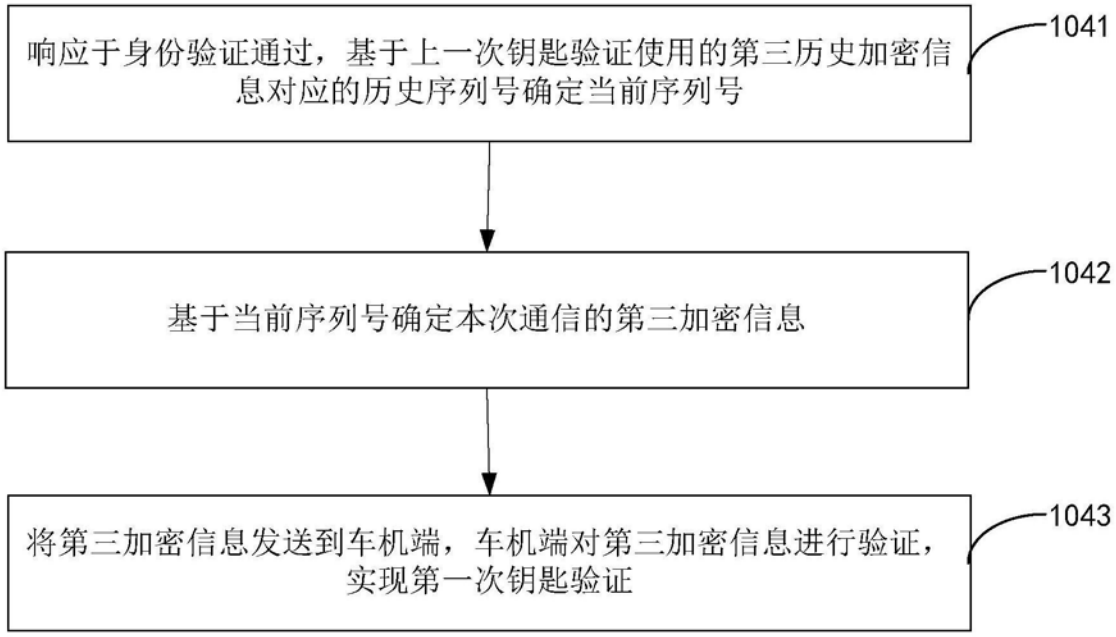

响应于身份验证通过，基于上一次钥匙验证使用的第三历史加密信息对应的历史序列号确定当前序列号
1041
基于当前序列号确定本次通信的第三加密信息
1042
将第三加密信息发送到车机端，车机端对第三加密信息进行验证，实现第一次钥匙验证
1043

图3

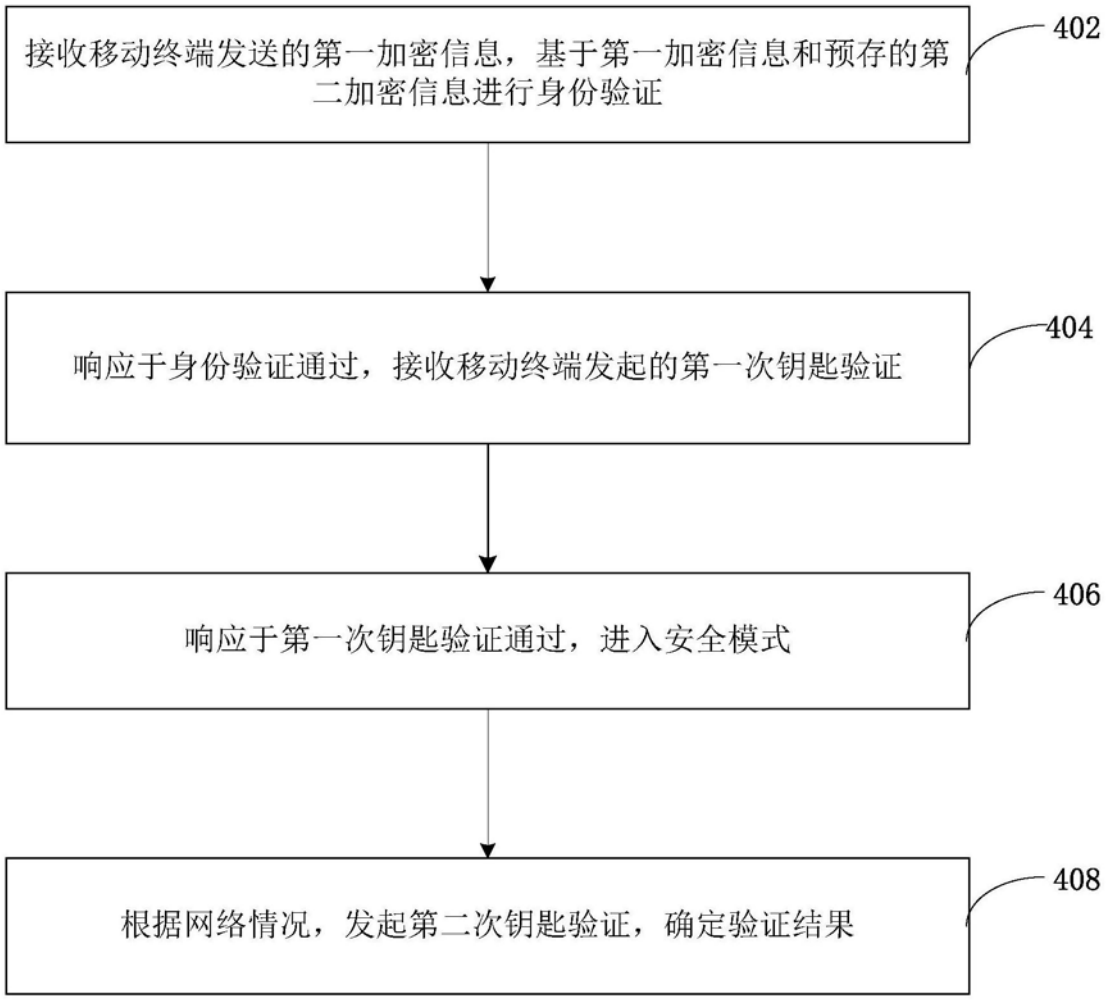

接收移动终端发送的第一加密信息，基于第一加密信息和预存的第二加密信息进行身份验证
402
响应于身份验证通过，接收移动终端发起的第一次钥匙验证
404
响应于第一次钥匙验证通过，进入安全模式
406
根据网络情况，发起第二次钥匙验证，确定验证结果
408

图4

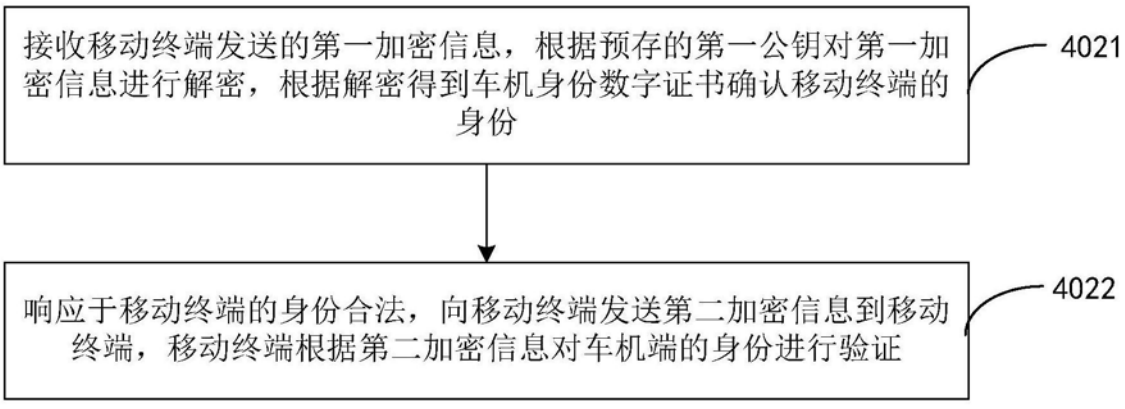

接收移动终端发送的第一加密信息，根据预存的第一公钥对第一加密信息进行解密，根据解密得到车机身份数字证书确认移动终端的身份
4021
响应于移动终端的身份合法，向移动终端发送第二加密信息到移动终端，移动终端根据第二加密信息对车机端的身份进行验证
4022

图5

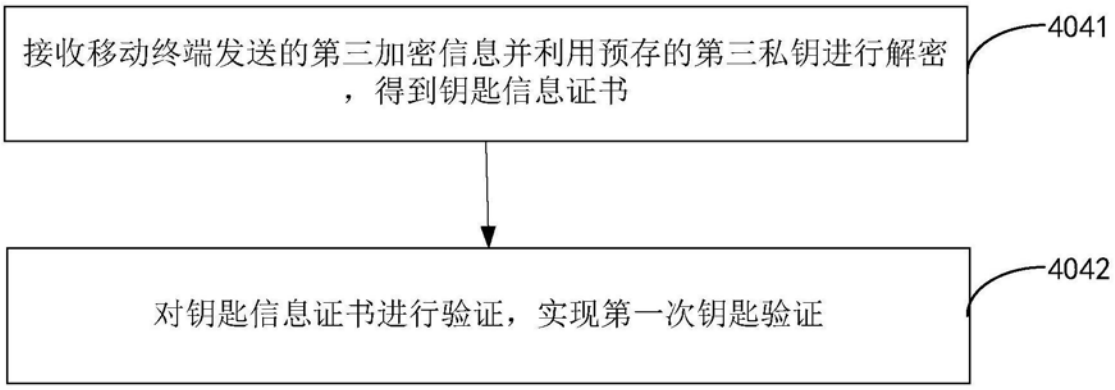

接收移动终端发送的第三加密信息并利用预存的第三私钥进行解密，得到钥匙信息证书
4041
对钥匙信息证书进行验证，实现第一次钥匙验证
4042

图6

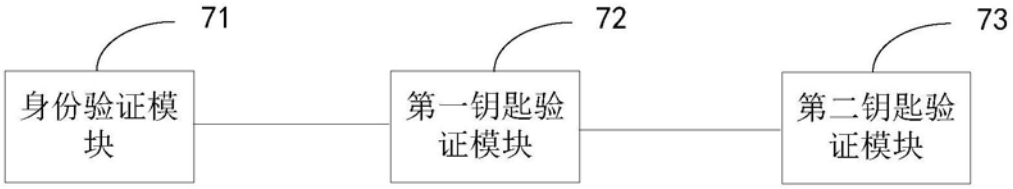

71
身份验证模块
72
第一钥匙验证模块
73
第二钥匙验证模块

图7

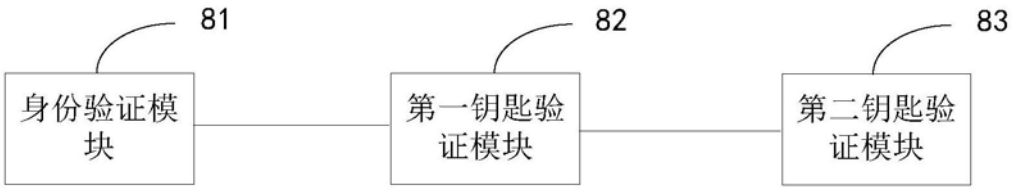

81
身份验证模块
82
第一钥匙验证模块
83
第二钥匙验证模块

图8

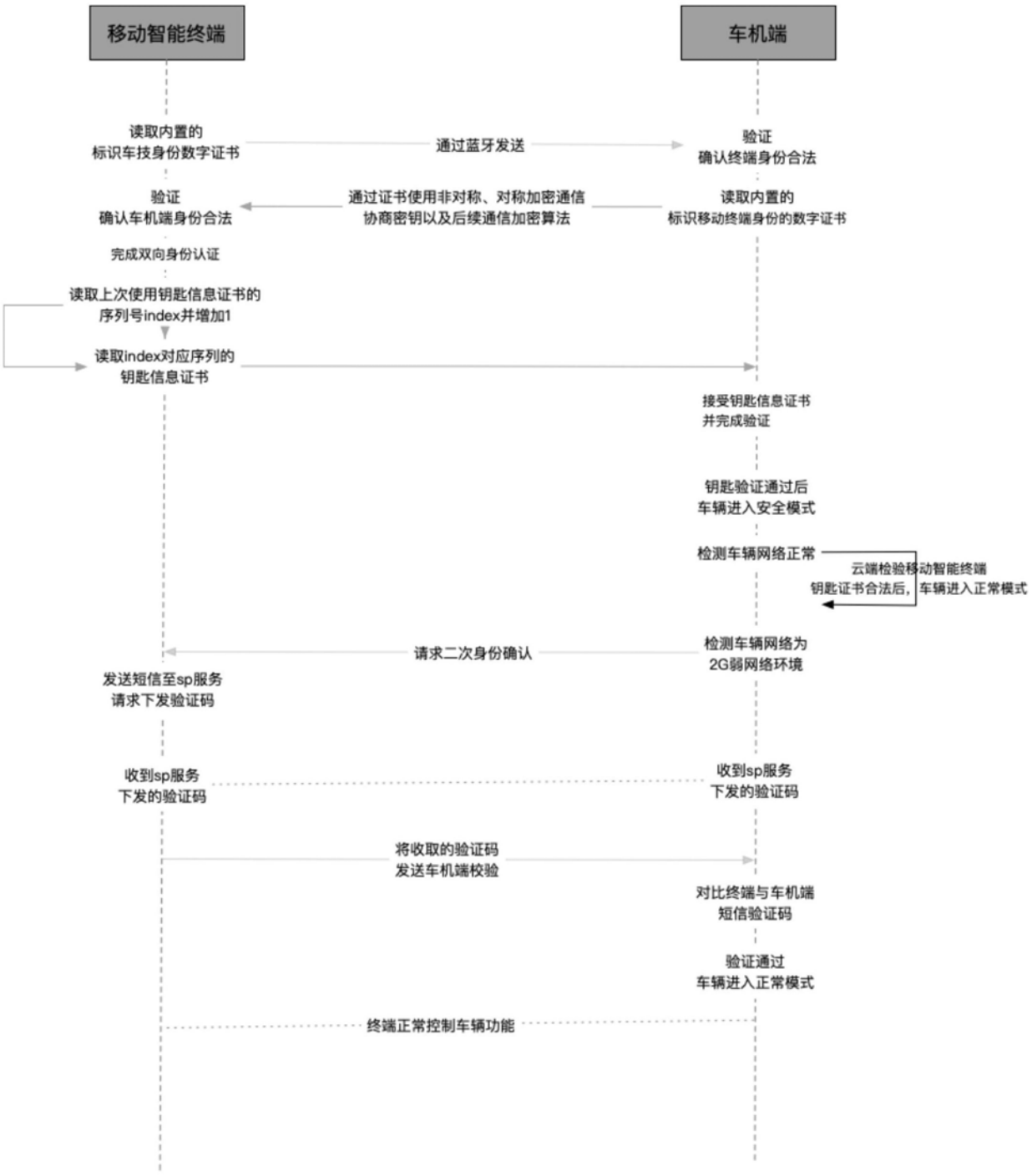

移动智能终端
车机端
读取内置的
标识车技身份数字证书
通过蓝牙发送
验证
确认终端身份合法
验证
确认车机端身份合法
通过证书使用非对称、对称加密通信
协商密钥以及后续通信加密算法
读取内置的
标识移动终端身份的数字证书
完成双向身份认证
读取上次使用钥匙信息证书的
序列号index并增加1
读取index对应序列的
钥匙信息证书
接受钥匙信息证书
并完成验证
钥匙验证通过后
车辆进入安全模式
检测车辆网络正常
云端检验移动智能终端
钥匙证书合法后，车辆进入正常模式
请求二次身份确认
检测车辆网络为
2G弱网络环境
发送短信至sp服务
请求下发验证码
收到sp服务
下发的验证码
收到sp服务
下发的验证码
将收取的验证码
发送车机端校验
对比终端与车机端
短信验证码
验证通过
车辆进入正常模式
终端正常控制车辆功能

图9