(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 110099037 B
(45)授权公告日 2021.10.01

(21)申请号 201811581311.6
(22)申请日 2013.07.16
(65)同一申请的已公布的文献号
申请公布号 CN 110099037 A
(43)申请公布日 2019.08.06
(30)优先权数据
61/672,463 2012.07.17 US
61/672,474 2012.07.17 US
13/942,367 2013.07.15 US
(62)分案原申请数据
201380035153.3 2013.07.16
(73)专利权人 德州仪器公司
地址 美国德克萨斯州
(72)发明人 何金梦 埃里克·佩特斯
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 林斯凯
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/50(2021.01)
G07C 9/00(2020.01)
审查员 焦伟

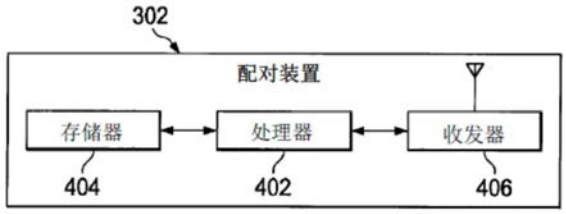
权利要求书2页 说明书7页 附图6页

(54)发明名称

基于证书的控制单元遥控钥匙配对

(57)摘要

本揭露涉及基于证书的控制单元遥控钥匙配对。一种遥控钥匙-控制单元配对装置(302)，其包含：收发器(406)，其用以发射及接收信号；存储器(404)，其用以存储与所述配对装置相关联的真实性证书(CertVD)及公共密钥PKVM；及处理器(402)，其耦合到所述收发器及存储器。所述处理器(402)经配置以：接收来自遥控钥匙且与所述遥控钥匙相关联的公共密钥PKKF及与所述遥控钥匙相关联的真实性证书CertKF；借助所述PKVM检验所述CertKF；及将经加密PKKF发射到控制单元。



CN 110099037 B

1.一种控制单元,其包括:

收发器;

存储器,以存储指令;及

处理器,其耦合到所述收发器和存储器,其中所述处理器经配置以执行所述指令,以使所述控制单元:

接收包含证书的第一发射;

检验所述证书的真实性;

在检验所述证书的真实性之后,使用收发器建立第一通信链路以执行公共密钥协商协议以产生第一共用秘密加密密钥;

接收包含经加密第一公共密钥的第二发射,其中所述经加密第一公共密钥通过所述第一共用秘密加密密钥被加密;

使用所述第一共用秘密加密密钥解密所述经加密第一公共密钥以确定所述第一公共密钥;

在确定所述第一公共密钥之后,使用所述收发器建立第二通信链路以执行公共密钥协商协议以产生第二共用秘密加密密钥;

产生操作密钥;

使用所述第二共用秘密加密密钥对所述操作密钥进行加密;及

发射经加密操作密钥。

2.如权利要求1所述的控制单元,其中所述证书与交通工具经销商相关联,并且检验所述证书的真实性是使用存储于所述存储器中的第二公共密钥执行的。

3.如权利要求2所述的控制单元,其中所述第一公共密钥与遥控钥匙装置相关联,所述控制单元经配置以被配对到所述遥控钥匙装置,且所述第二公共密钥与交通工具制造商相关联。

4.如权利要求1所述的控制单元,其中检验所述证书的真实性包含确定所述证书不在证书撤销列表上。

5.如权利要求1所述的控制单元,其中所述操作密钥以随机数的方式生成。

6.如权利要求5所述的控制单元,其中所述随机数为128位随机数。

7.如权利要求1所述的控制单元,其中通过建立所述第一通信链路和所述第二通信链路执行的所述公共密钥协商协议中的至少一者为椭圆曲线迪菲-赫尔曼(ECDH)密钥协商协议或椭圆曲线密码术(ECC)密钥协商协议。

8.如权利要求1所述的控制单元,其中至少部分基于所述第一公共密钥而建立所述第二通信链路。

9.如权利要求8所述的控制单元,其中包含于所述第一公共密钥中的所述信息识别遥控钥匙装置,所述控制单元经配置以被配对到所述遥控钥匙装置。

10.一种产生经加密的操作密钥的方法,所述方法包括:

接收包含证书的第一发射;

检验所述证书的真实性;

在检验所述证书的真实性之后,执行公共密钥协商协议以产生第一共用秘密加密密钥;

接收包含经加密第一公共密钥的第二发射，其中所述经加密第一公共密钥通过所述第一共用秘密加密密钥被加密；

使用所述第一共用秘密加密密钥以解密所述经加密第一公共密钥；

在确定所述第一公共密钥之后，执行公共密钥协商协议以产生第二共用秘密加密密钥；

产生操作密钥；

使用所述第二共用秘密加密密钥对所述操作密钥进行加密；及

发射经加密操作密钥。

11.如权利要求10所述的方法，其中检验所述证书的真实性包括使用第二公共密钥。

12.如权利要求11所述的方法，其中：

所述证书与交通工具经销商相关联；

所述第一公共密钥与遥控钥匙装置相关联，控制单元经配置以被配对到所述遥控钥匙装置；及

所述第二公共密钥与交通工具制造商相关联。

13.如权利要求10所述的方法，其中检验所述证书的真实性包含确定所述证书不在证书撤销列表上。

14.如权利要求10所述的方法，其中所述操作密钥以随机数的方式生成。

15.如权利要求14所述的方法，其中所述随机数为128位随机数。

16.如权利要求10所述的方法，其中被执行以产生所述第一共用秘密加密密钥的所述公共密钥协商协议和被执行以产生所述第二共用秘密加密密钥的所述公共密钥协商协议中的至少一者为椭圆曲线迪菲-赫尔曼(ECDH)密钥协商协议或椭圆曲线密码术(ECC)密钥协商协议中的一者。

基于证书的控制单元遥控钥匙配对

[0001] 本申请是申请日为2013年07月16日，申请号为“201380035153.3”，而发明名称为“基于证书的控制单元遥控钥匙配对”的申请的分案申请。

背景技术

[0002] 无线遥控钥匙及其相应交通工具可使用经加密操作密钥来验证在所述两者之间发生的通信。为了使遥控钥匙与交通工具能够通信，必须在制造或销售过程中的某一时刻对其进行配对。无线遥控钥匙与其相应交通工具的配对按惯例要求交通工具制造商向各种交通工具经销商递送与每一遥控钥匙相关联的秘密密钥，其中所述秘密密钥为密码密钥。可接着使用遥控钥匙的秘密密钥来使遥控钥匙与交通工具相关联，或将遥控钥匙与交通工具配对。通常，将多个遥控钥匙与每一交通工具配对。然而，此向交通工具经销商递送秘密密钥的步骤可能给秘密密钥的盗窃开放了导致未经授权遥控钥匙及潜在盗窃的途径，且这些遥控钥匙中的每一者必须存储秘密密钥的事实开放所述途径。

发明内容

[0003] 上文所述的问题在很大程度上通过一种遥控钥匙-控制单元配对装置来解决，所述配对装置包含：收发器，其用以发射及接收信号；存储器，其用以存储与所述配对装置相关联的真实性证书(CertVD)及公共密钥(PKVM)；及处理器，其耦合到所述收发器及存储器。所述处理器用以：接收来自遥控钥匙且与所述遥控钥匙相关联的公共密钥(PKKF)及与所述遥控钥匙相关联的真实性证书(CertKF)；借助所述PKVM检验所述CertKF；及将经加密PKKF发射到控制单元。

[0004] 所述解决方案还可涉及一种遥控钥匙，其包含：收发器，其用以接收及发送信号；存储器，其用以存储与所述遥控钥匙相关联的公共密钥(PKKF)及真实性证书(CertKF)；及处理器，其耦合到所述收发器及存储器。所述处理器用以：将所述PKKF及所述CertKF发射到配对装置；执行公共密钥协商协议以产生共用秘密加密密钥；及从控制单元接收借助所述共用秘密加密密钥加密的操作密钥。

[0005] 以上问题的另一解决方案可为一种用以将遥控钥匙与交通工具的控制单元配对的方法，其包含：由配对装置从遥控钥匙读取公共加密密钥(PKKF)及真实性证书(CertKF)；由所述配对装置使用交通工具制造商的公共加密密钥(PKVM)检验所述CertKF；由所述配对装置将真实性证书(CertVD)发射到控制单元；由所述控制单元使用所述PKVM检验所述CertVD；由所述配对装置及所述控制单元执行公共密钥协商以产生加密密钥DHKey1；由所述配对装置使用所述DHKey1将所述PKKF加密；由所述配对装置将所述经加密PKKF发射到所述控制单元；由所述控制单元及所述遥控钥匙执行公共密钥协商以产生加密密钥DHKey2；由所述控制单元使用所述DHKey2将操作密钥加密；及由所述控制单元将所述经加密操作密钥发射到所述遥控钥匙。

附图说明

[0006] 图1展示根据如本文中所论述的各种实例从子单元制造到交通工具经销商实施基于证书的验证遥控钥匙-控制单元配对的实例性交通工具制造流程；

[0007] 图2是根据如本文中所描述的各种实例用于基于证书的验证的实例性遥控钥匙与控制单元预配对调节过程；

[0008] 图3展示根据如本文中所论述的各种实施例使用基于证书的验证对控制单元与遥控钥匙的初始配对过程的实例；

[0009] 图4是根据本文中所论述的各种实例的实例性配对装置的框图；

[0010] 图5是根据本文中所论述的各种实例的实例性遥控钥匙的框图；

[0011] 图6是根据本文中所论述的各种实例的实例性控制单元的框图；

[0012] 图7展示根据如本文中所论述的各种实例的在配对之后的经配对遥控钥匙与控制单元的实例性操作；

[0013] 图8展示根据如本文中所论述的各种实例的由CU进行的操作密钥改变的实例；

[0014] 图9是根据本文中所论述的各种实例用于基于证书的验证的方法的实例性流程图；且

具体实施方式

[0015] 遥控钥匙与交通工具(例如，汽车、摩托车、船、小型摩托车等)的配对可需要安全信息的输送及使用以确保假冒遥控钥匙不与交通工具配对，假冒遥控钥匙与交通工具的配对可导致盗窃。所述完整常规过程可由交通工具制造商保密以确保其交通工具的安全性。然而，此过程可要求制造商开发昂贵且专用IT系统来产生秘密密钥且维持其安全性。然而，当交通工具被递送到代理商时，秘密密钥被传递下去使得可在最后目的地处对多个遥控钥匙进行配对。秘密密钥从制造商到经销商的输送可呈现导致伪劣及假冒遥控钥匙的秘密密钥被盗的机会。

[0016] 除交通工具之外，所揭示方法还可用于将遥控钥匙与允许无线连接性及控制的任何类型的控制单元配对。例如，所揭示技术及装置可为车库门系统、酒店入口系统或家庭的远程进入的部分。如此，本发明的范围不限于交通工具的控制单元。交通工具及遥控钥匙与交通工具的一个或所有控制单元的配对的使用主要出于描述性目的。

[0017] 本文中揭示用于将遥控钥匙与交通工具配对的装置及方法，其可避免秘密信息向代理商的输送且可减少交通工具制造商的IT要求。一种方法(基于证书的验证过程)可涉及使用与在配对过程中所涉及的各种组件及行动者相关联的经验证证书及公共/私密密钥对。在基于证书的方法中，配对装置可从相关联遥控钥匙接收公共密钥及证书。所述配对装置还可由交通工具控制单元验证并在配对装置与控制单元之间建立秘密密钥。所述配对装置可接着借助秘密密钥将遥控钥匙的公共密钥加密并将经加密公共密钥发射到控制单元。控制单元可接着知晓将与何种遥控钥匙配对。所述控制单元及遥控钥匙可接着产生待在其自身之间使用的另一秘密密钥，所述另一秘密密钥可接着由控制单元用以将操作密钥加密。可接着将经加密操作密钥传达到遥控钥匙以便将两个装置配对。

[0018] 用以将遥控钥匙与控制单元配对的基于证书的方法可涉及所有行动者(制造商、组装者、经销商等)获得公共及秘密(私密)加密密钥，所述加密密钥可用以在配对过程中彼

此验证。这可意味着每一交通工具经销商(或经销商/配对装置)、交通工具制造商、制造及组装的每一遥控钥匙及制造并安装于交通工具中的每一控制单元将具有其自身的相关联公共/秘密密钥对。一旦所涉及的组件已获取其密钥对,便可由可信的第三方或证书授权机构(CA)认证公共密钥。所述CA可从相关联组件接收公共密钥及标识以证明其识别码。在其识别码被证明之后,CA可接着借助可信第三方的秘密密钥来签署所述方的公共密钥。经签署公共密钥变为请求方的真实性证书。为了检验证书的识别码,另一方需要使用可信第三方的公共密钥将证书解锁。举例来说,所述CA可为交通工具制造商或由汽车制造商指定的第三方。

[0019] 各种组件(遥控钥匙、配对装置及控制单元)可使用某些公共/秘密密钥及证书来彼此验证且产生将用于在彼此之间传递信息的秘密加密密钥。秘密密钥的产生可使用公共密钥协商协议,例如椭圆曲线迪菲-赫尔曼(Diffie-Hellman)(ECDH)或椭圆曲线密码术(ECC)。作为配对过程的部分,一对组件(例如遥控钥匙与控制单元)可使用秘密加密密钥。

[0020] 图1展示根据如本文中所论述的各种实例从子单元制造到交通工具经销商实施基于证书的验证遥控钥匙-控制单元配对的实例性交通工具制造流程100。流程100可包含遥控钥匙制造商102、遥控钥匙组装104(展示潜在地多个层中的层1)、控制单元(CU)制造商106、CU组装108(展示潜在地多个层中的层1)、交通工具制造商110及交通工具经销商112。流程100展示最终可经配对以用于操作及进入到对应交通工具中的组件的进展。每一交通工具可具有多个CU,其中每一CU控制不同功能,即,点火、制动、进入、行李厢等。个别遥控钥匙可与对应交通工具的一个、几个或所有CU配对。另外,每一交通工具及各种数目的CU可与多个遥控钥匙配对。此外,与交通工具相关联的每一遥控钥匙可在丢失或被盗的情况下被去激活,而不会影响与所述同一交通工具相关联的任何其它遥控钥匙。

[0021] 每一遥控钥匙可具有指派给其且存储在内部的公共密钥(PK_{KF})与秘密密钥(SK_{KF})对。可由遥控钥匙制造商102、遥控钥匙组装104或交通工具制造商110针对每一遥控钥匙产生PK_{KF}/SK_{KF}对并安装于所述每一遥控钥匙中。交通工具制造商110可选择最可信的实体来产生及安装PK_{KF}/SK_{KF}对以确保秘密性及安全性。这同样适用于经制造并安装于交通工具中的每一控制单元-每一控制单元将具有由可信方(CU制造商106、CU组装108或交通工具制造商110)产生并安装到相关联CU中的密钥对(PK_{CU}/SK_{CU})。

[0022] 除遥控钥匙及CU包含其相应PK/SK对之外,每一单元还可包含验证组件的识别码的真实性证书(Cert)。按惯例,Cert为经检验及签署的公共密钥,其中Cert由CA签署。CA可借助其秘密密钥签署Cert。出于安全性原因,交通工具制造商110可为可信的第三方,因此其可控制制造及遥控钥匙-汽车配对过程中的流程及Cert有效性。如此,交通工具制造商110可借助其秘密密钥(SK_{VM})签署所有公共密钥以产生对应证书。举例来说,$Cert_{KF}$将被插入到相关联遥控钥匙中。$Cert_{CU}$可对应于CU。

[0023] 交通工具经销商112还可获得密钥对(PK_{VD}及SK_{VD})以便在遥控钥匙-CU配对过程中加以检验。交通工具经销商112的密钥对(及也由交通工具制造商110签署的相关联$Cert_{VD}$)可与经销商配对装置或简单地配对装置相关联。为论述简明起见,遥控钥匙-汽车配对将描述为在交通工具经销商112处发生,但所述配对还可在交通工具制造商110处发生而不偏离本发明的界限。

[0024] 在任何遥控钥匙-CU配对可开始之前,一些调节步骤可在各种制造及/或组装位置

处发生。所述调节可经执行以准备好单独的组件(遥控钥匙、CU、经销商(配对装置)),使得配对功能为既定的。然而,可连续地进行调节及配对步骤。举例来说,如果如本文中所描述,在交通工具经销商112处执行配对,那么调节可在交通工具制造商110处发生。

[0025] 图2是根据如本文中所描述的各种实例用于基于证书的验证的实例性遥控钥匙与控制单元预配对调节过程200。调节过程200可涉及交通工具制造商110、交通工具经销商112、CU 202及遥控钥匙204。调节过程200的步骤是以某一次序展示,但对所述次序的改变在本发明的范围内。所展示的次序仅出于说明性目的。调节过程200的目标可为调节或准备好相应组件以促进遥控钥匙与CU的初始配对,此可在交通工具制造商110的位置处或在交通工具经销商112处发生。

[0026] 调节过程200可在步骤1a处以交通工具经销商112产生其加密密钥对(PK_{VD}及SK_{VD},如上文所论述)而开始。经销商112可接着将其PK_{VD}以真实方式发射到交通工具制造商110。以真实方式发射可向交通工具制造商110确保交通工具经销商112的识别码,且真实发射可为物理上邮寄PK_{VD}或通过快递员或某一其它形式的经检验发射递送PK_{VD}。在接收到PK_{VD}后,交通工具制造商110可接着通过借助交通工具制造商110的秘密密钥SK_{VM}签署PK_{VD}来认证PK_{VD},从而为交通工具经销商112产生真实性证书($Cert_{VD}$)。交通工具制造商110接着将$Cert_{VD}$发送回到经销商112,$Cert_{VD}$可被插入到经销商的相关联配对装置中。

[0027] 调节过程200还可包含交通工具制造商110将其公共密钥PK_{VM}插入到每一交通工具的CU202中且还插入到每一遥控钥匙204中。插入到遥控钥匙204及CU 202中的PK_{VM}可在稍后时间用以检验另一装置的真实性/识别码,因为所有真实性证书应由交通工具制造商110签署,这可使用PK_{VM}来检验。

[0028] 最后,作为调节过程200的部分,经销商112可读取每一遥控钥匙204的PK_{KF},其并非秘密的。经销商可一次接收众多遥控钥匙204且可决定立刻读取所有其相关联公共密钥以存储在配对装置中。或者,作为初始配对过程的部分,经销商112可读取单个遥控钥匙的PK_{KF},下文将描述。

[0029] 图3展示根据如本文中所论述的各种实施例使用基于证书的验证对控制单元与遥控钥匙的初始配对过程300的实例。初始配对过程300可在交通工具制造商的位置处或如所展示在交通工具经销商处发生。初始配对过程300可包含交通工具制造商110、与交通工具经销商112相关联的配对装置302、遥控钥匙204及CU 202。配对装置302可能已含有PK_{VM},两者均可用以检验其它组件(CU 202及遥控钥匙204)的识别码。配对装置302可经由无线连接(例如借助蓝牙、超高频(UHF)或低频(LF))与遥控钥匙204及控制单元202通信,或其可经由导线连接。组件之间的无线及有线连接均在本发明的范围内。另外或替代地,配对装置302可与一个组件(例如,遥控钥匙204)无线地通信且经由导线与另一组件(例如,CU 202)通信。

[0030] 此外,配对装置302可为手持式装置、固定终端或交通工具经销商112或交通工具制造商110(取决于配对过程将在何处发生)的安全位置中的安全计算机。在任一实施例中,配对装置302可具有与交通工具制造商110的安全通信信道。安全通信信道可为永久连接或可经周期性地建立(例如,每夜)以更新列表并接收安全通信。

[0031] 初始配对过程300可通过配对装置302从遥控钥匙204接收与遥控钥匙相关联的PK_{KF}及$Cert_{KF}$而开始,步骤1a。可由于由配对装置302发送的请求而将信息从遥控钥匙204发

送到配对装置302。或者，遥控钥匙204可周期性地广播其PK_{KF}及$Cert_{KF}$。配对装置302可接着通过检验Cert KF的真实性而检验遥控钥匙204的识别码，步骤1b。$Cert_{KF}$可由配对装置使用所存储PK_{VM}来检验。可通过将$Cert_{KF}$与PK_{VM}进行散列运算来执行$Cert_{KF}$的检验。

[0032] 如果配对装置302不能够检验$Cert_{KF}$，那么可将与所述$Cert_{KF}$相关联的遥控钥匙204视为伪劣品且停止进一步的配对步骤。另外或替代地，配对装置302可检验所接收$Cert_{KF}$不在由交通工具制造商110维持的证书撤销列表(CRL)上，步骤1c。此检验步骤可确保特定$Cert_{KF}$在之前尚未被多次使用，被多次使用可用信号通知欺骗性的遥控钥匙。所述CRL可存储于配对装置302的存储器中且经周期性地更新，或配对装置302可不断地存取在交通工具制造商110处的服务器上维持的CRL。

[0033] 配对装置302可在检验遥控钥匙204之前、之后或与之同时地开始与CU 202的通信，使得CU 202可检验配对装置302的识别码。配对装置302将其$Cert_{VD}$发送到CU 202，步骤2a。CU 202使用PK_{VM}检验$Cert_{VD}$的真实性。另外或替代地，CU 202可检验$Cert_{VD}$不在也由交通工具制造商110维持的CRL上。举例来说，CU 202可使用交通工具经销商112处的无线接入点来接入因特网及交通工具制造商110处的服务器以确定$Cert_{VD}$是否在撤销列表上。

[0034] 如果$Cert_{VD}$为无法检验的或在CRL上，那么CU 202可确定配对装置302及/或经销商112为欺骗性的。如果被视为欺骗性的，那么CU 202可终止与配对装置302通信且可警示交通工具制造商110。

[0035] 如果CU 202能够检验配对装置302，那么CU 202及配对装置302两者执行密钥协商协议以产生可仅被配对装置302及CU 202知晓的共用秘密密钥DHKey1，步骤3a。在产生DHKey1之后，配对装置302可将遥控钥匙202的PK_{KF}加密并将经加密PK_{KF}发射到CU 202。由于CU 202知晓DHKey1且可将揭露PK_{KF}的消息解密，因此CU 202知晓将与何种遥控钥匙204通信及配对。

[0036] CU 202可经由无线方式直接地或通过配对装置302起始与遥控钥匙202的通信。一旦在遥控钥匙204与CU 202之间建立通信链路，两个组件202、204便可执行密钥协商协议以产生仅被CU 202及遥控钥匙204知晓的共用秘密密钥DHKey2，步骤4a。CU 204可接着产生操作密钥(OpKey)，使用DHKey2将OpKey加密并将经加密OpKey发射到遥控钥匙204，步骤4b。OpKey可为随机产生的128位数。

[0037] 遥控钥匙204可接着将消息解密以获悉OpKey。此时，可将遥控钥匙204及CU 202视为配对的且正常操作可开始。遥控钥匙204及CU 202可使用OpKey基于任何标准私密或公共密钥验证技术(例如，ISO 9798-2)在正常操作中彼此验证。

[0038] 还可使用基于标识(ID)的验证方法来执行将遥控钥匙与控制单元配对。基于ID的方法可使用与遥控钥匙及CU相关联的可用于既彼此验证又产生装置之间的秘密密钥的唯一标识字。所述秘密密钥将接着用以将在两个组件之间发送的信息加密及解密。再次，遥控钥匙与CU的配对可由位于交通工具经销商处或位于交通工具制造商处且可类似于配对装置302的配对装置来促进。

[0039] 图4、5及6分别展示根据本文中所论述的各种实例的实例性配对装置302、遥控钥匙204及CU 202的框图。三个装置/组件-配对装置、遥控钥匙及CU-均可包括处理器(402、502、602)，存储器(404、504、604)及收发器(406、506、606)。三个装置/组件的处理器可用于执行与基于证书的验证配对及基于ID的验证配对相关联的验证计算及共用秘密密钥产生

计算。处理器可为标准CPU、微控制器、低功率数字信号处理器等且可能够在短时间内执行复杂计算。

[0040] 三个装置的存储器可用于存储公共与私密密钥对及与其用于基于证书的验证配对的相应装置相关联的真实性证书。替代地或另外，三个装置的存储器可用于存储其自身或其它装置的ID。举例来说，在基于ID的验证配对中，配对装置302可在起始配对序列之前存储KFID及CUID两者。用于那两个相关联装置的KFID及CUID可存储于配对装置302的存储器404中。存储器可为非易失性存储装置，例如快闪存储器或EEPROM。

[0041] 用于三个装置的收发器可为有线的(未展示)、无线的或能够进行两者。收发器可由装置用以在用于任一验证方法的调节步骤及初始配对步骤期间传达ID、公共密钥及/或真实性证书。允许交通工具的远程进入与控制的遥控钥匙可使用无线技术(例如，蓝牙、LF或UHF)进行那些发射，但还可能够在初始配对过程期间经由导线与配对装置及/或CU通信。

[0042] 另外，配对装置302可包含到交通工具制造商110的有线连接使得配对装置302可安全地接收递送到经销商112的CU 202的CUID以用于基于ID的验证配对。对于基于证书的验证配对，配对装置302可在存取证书撤销列表时与交通工具制造商110通信。另外，CU 202还可在检查配对装置302的CertVD的有效性时经由配对装置302或某一其它连接存取交通工具制造商110处的CRL。

[0043] 图7展示根据如本文中所论述的各种实例的经配对遥控钥匙与CU的实例性正常操作。图9中所描绘的正常操作展示遥控钥匙204与CU 202在通过过程300(基于证书)的初始配对之后的互动。遥控钥匙与CU在于用户与遥控钥匙(举例来说)的互动时彼此通信时，可通过基于AES-128(举例来说)执行OpKey验证质询-响应协议而首先彼此验证。遥控钥匙对CU的操作可仅在响应有效时被允许。无效响应可表示伪劣遥控钥匙，且CU可不执行从无效遥控钥匙发送的命令。

[0044] 图8展示根据如本文中所论述的各种实例由CU进行的OpKey改变的实例。CU 202可在遥控钥匙206被错放或被盗时改变OpKey。通过改变OpKey，CU可防止丢失或被盗的遥控钥匙206接入CU 202。CU 202可通过期望新OpKey的外部信号起始。外部信号可通过执行与其余遥控钥匙204及交通工具的预设置序列而来自所述遥控钥匙的所有者，或外部信号可来自经销商112的配对装置302。在接收到外部信号后，CU 202可即刻使用旧OpKey将新OpKey加密且接着将经加密新OpKey发射到其余遥控钥匙204。在接收到新OpKey之后，可由所有CU 202及其余遥控钥匙204将旧OpKey擦除。装置之间的正常操作可接着继续而无需担心伪劣遥控钥匙可与CU互动。

[0045] 图9是根据本文中所论述的各种实例用于基于证书的验证的实例性方法900的流程图。方法900A可为关于图3所描述的初始配对过程300的一个实施方案。方法900在步骤902处以配对装置302从遥控钥匙204读取公共加密密钥(PK_{KF})及真实性证书($Cert_{KF}$)而开始。方法900在步骤904处以配对装置302使用交通工具制造商110的公共加密密钥(PK_{VM})检验$Cert_{KF}$而继续。步骤906以配对装置302将真实性证书($Cert_{VD}$)发射到CU 202而使方法900继续。在步骤908处，CU 202使用可存储于CU 202的存储器804中的PK_{VM}检验$Cert_{KF}$。在步骤910处，配对装置302及CU 202执行公共密钥协商协议以产生可仅被配对装置及CU知晓的共用秘密加密密钥DHKey1。

[0046] 方法900接着在步骤912处以配对装置302使用DHKey1将PK_{KF}加密而继续，之后方法

900以配对装置302将经加密PK_{KF}发射到控制单元202而执行步骤914。在步骤916处，CU 202及遥控钥匙204执行公共密钥协商协议以产生待在CU 202与遥控钥匙204之间共享的共用秘密加密密钥DHKey2。方法900以步骤918及920结束，其中CU 202借助DHKey2将操作密钥(OpKey)加密且接着将经加密OpKey发射到遥控钥匙204。在已将OpKey与遥控钥匙204共享之后，可将CU 202及遥控钥匙204视为配对的。

[0047] 所属领域的技术人员将了解，在所主张发明的范围内，可对所描述实施例做出修改，并且许多其它实施例也为可能的。

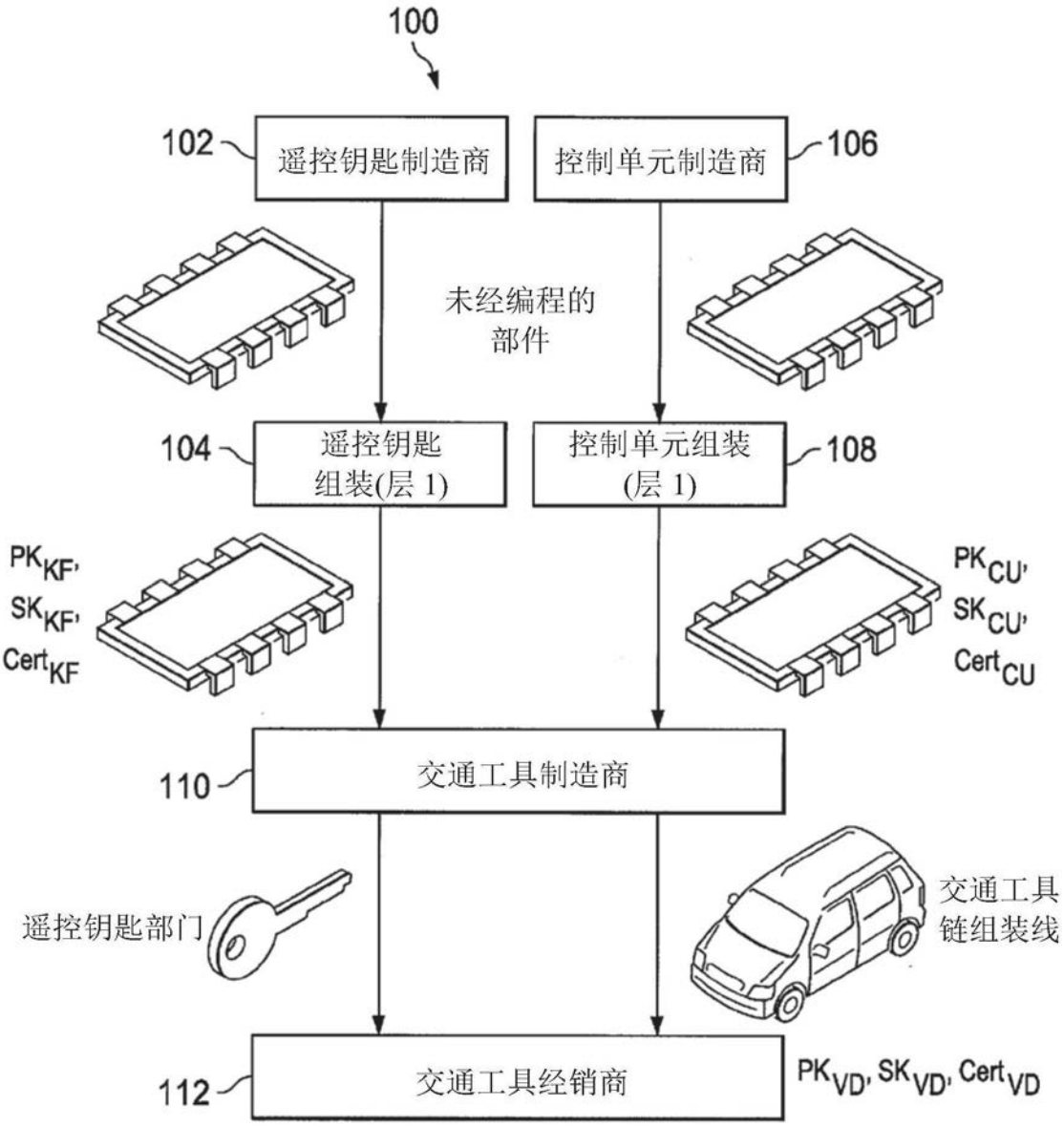

100
102
遥控钥匙制造商
控制单元制造商
106
未经编程的
部件
104
遥控钥匙
组装(层 1)
控制单元组装
(层 1)
108
PK_KF,
SK_KF,
Cert_KF
PK_CU,
SK_CU,
Cert_CU
110
交通工具制造商
遥控钥匙部门
交通工具
链组装线
112
交通工具经销商
PK_VD, SK_VD, Cert_VD

图1

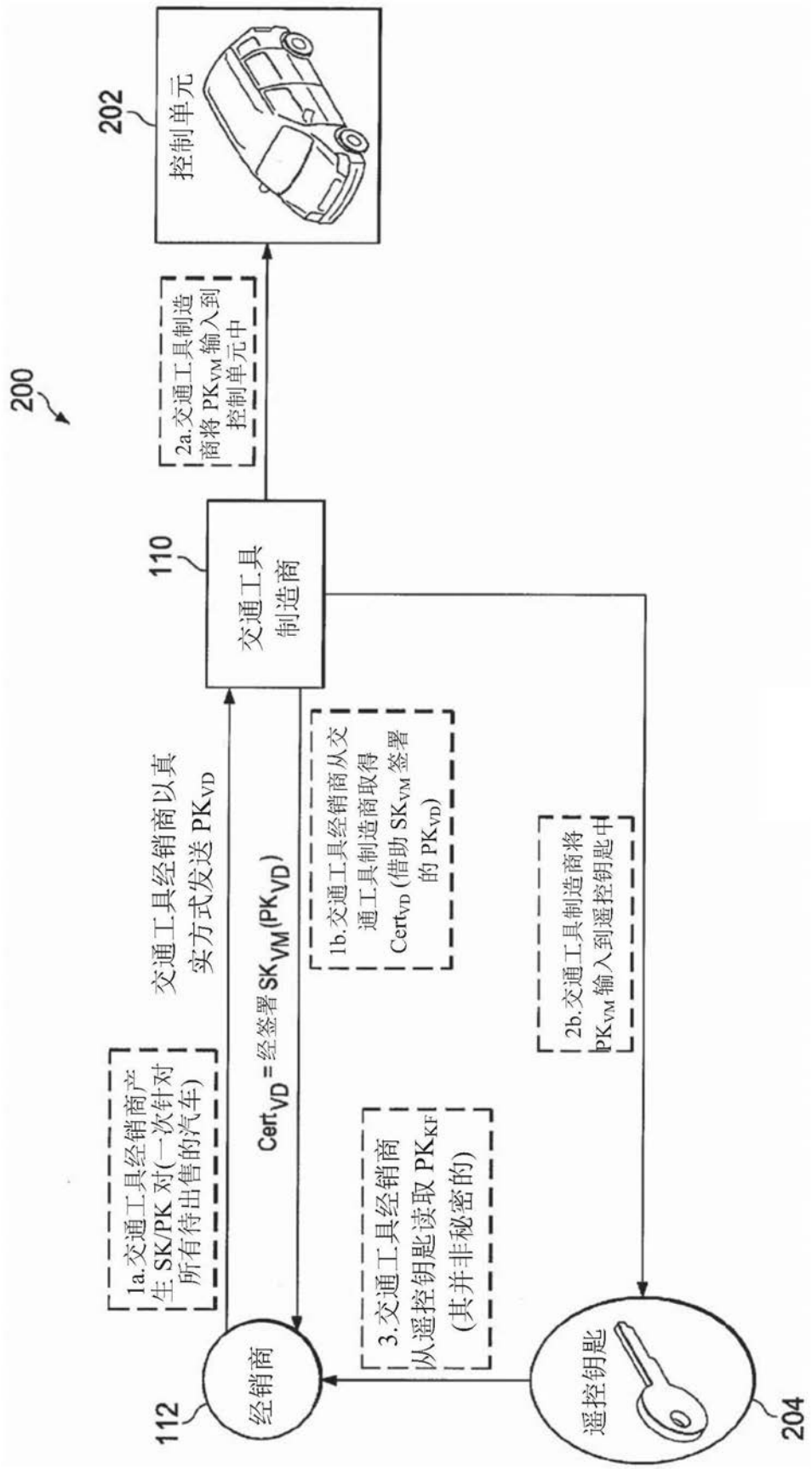

200
202
控制单元
2a.交通工具制造商将 PK_{VM} 输入到控制单元中
110
交通工具制造商
交通工具经销商以真实方式发送 PK_{VD}
$Cert_{VD}$ = 经签署 $SK_{VM}(PK_{VD})$
1b.交通工具经销商从交通工具制造商取得 $Cert_{VD}$ (借助 SK_{VM} 签署的 PK_{VD})
1a.交通工具经销商产生 SK/PK 对(一次针对所有待出售的汽车)
2b.交通工具制造商将 PK_{VM} 输入到遥控钥匙中
3.交通工具经销商从遥控钥匙读取 PK_{KF} (其并非秘密的)
112
经销商
遥控钥匙
204

图2

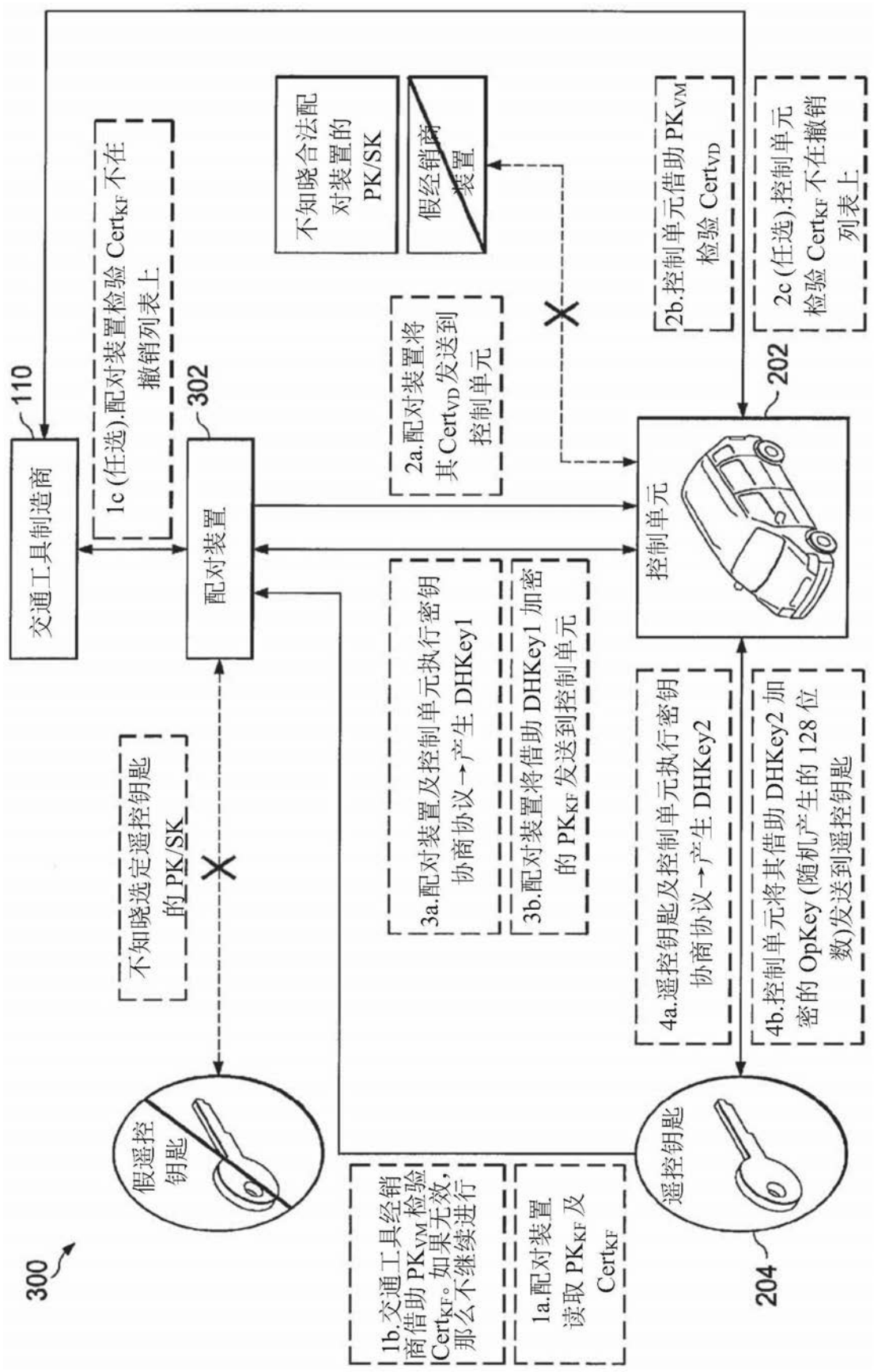

300
交通工具制造商
110
配对装置
302
控制单元
202
假遥控钥匙
遥控钥匙
204
1a.配对装置读取 PK_{KF} 及 $Cert_{KF}$
1b.交通工具经销商借助 PK_{VM} 检验 $Cert_{KF}$。如果无效，那么不继续进行
不知晓选定遥控钥匙的 PK/SK
1c (任选).配对装置检验 $Cert_{KF}$ 不在撤销列表上
不知晓合法配对装置的 PK/SK
假经销商装置
2a.配对装置将其 $Cert_{VD}$ 发送到控制单元
2b.控制单元借助 PK_{VM} 检验 $Cert_{VD}$
2c (任选).控制单元检验 $Cert_{KF}$ 不在撤销列表上
3a.配对装置及控制单元执行密钥协商协议→产生 DHKey1
3b.配对装置将借助 DHKey1 加密的 PK_{KF} 发送到控制单元
4a.遥控钥匙及控制单元执行密钥协商协议→产生 DHKey2
4b.控制单元将其借助 DHKey2 加密的 OpKey (随机产生的 128 位数)发送到遥控钥匙

图3

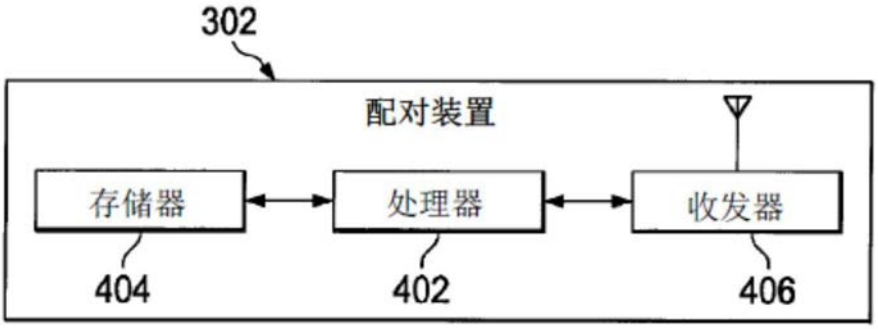

302
配对装置
存储器
处理器
收发器
404
402
406

图4

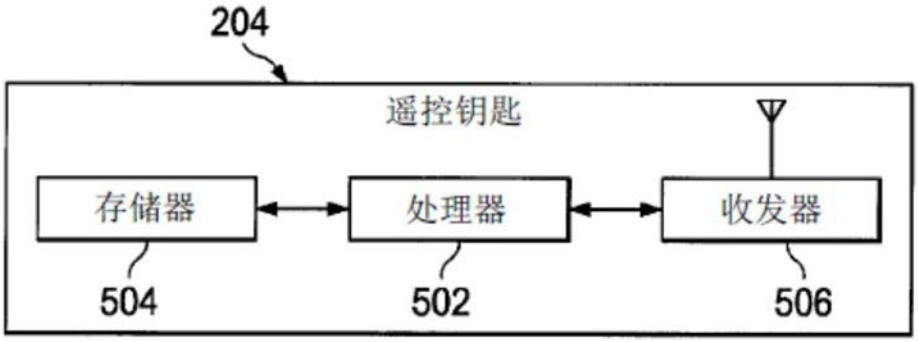

204
遥控钥匙
存储器
处理器
收发器
504
502
506

图5

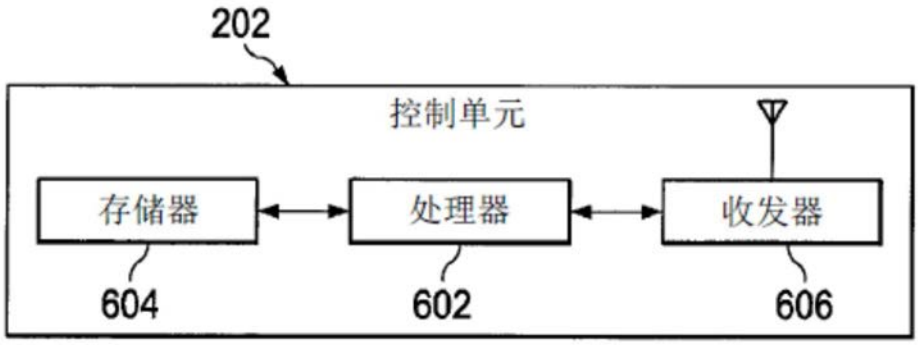

202
控制单元
存储器
处理器
收发器
604
602
606

图6

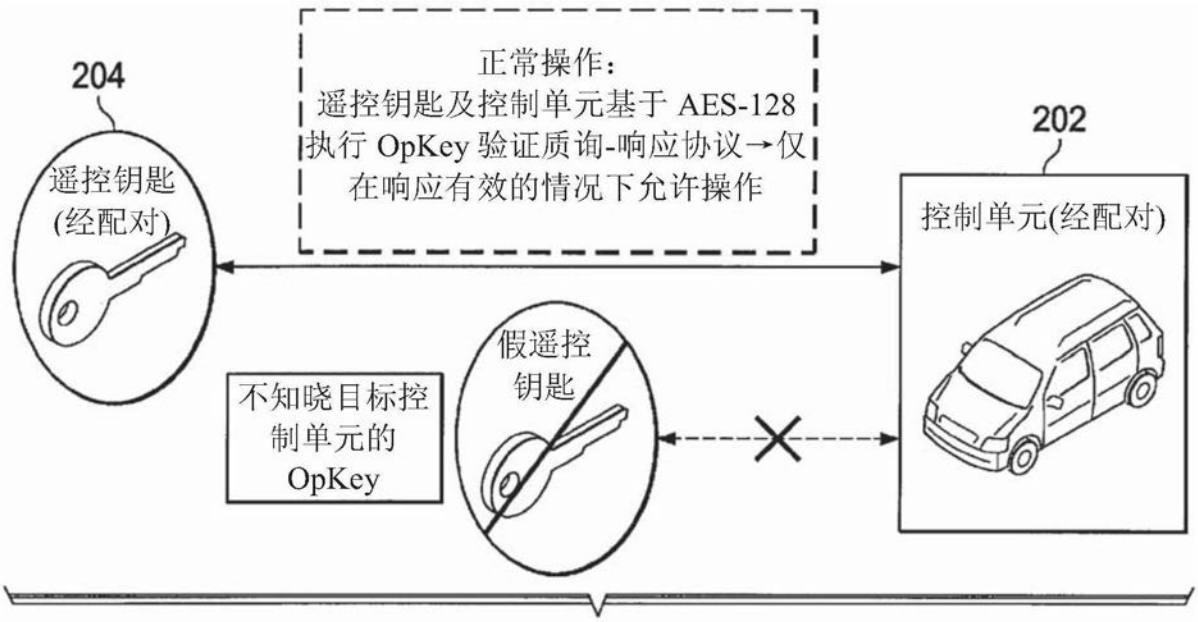

204
遥控钥匙
(经配对)
正常操作：
遥控钥匙及控制单元基于 AES-128
执行 OpKey 验证质询-响应协议→仅
在响应有效的情况下允许操作
202
控制单元(经配对)
不知晓目标控
制单元的
OpKey
假遥控
钥匙

图 7

图7

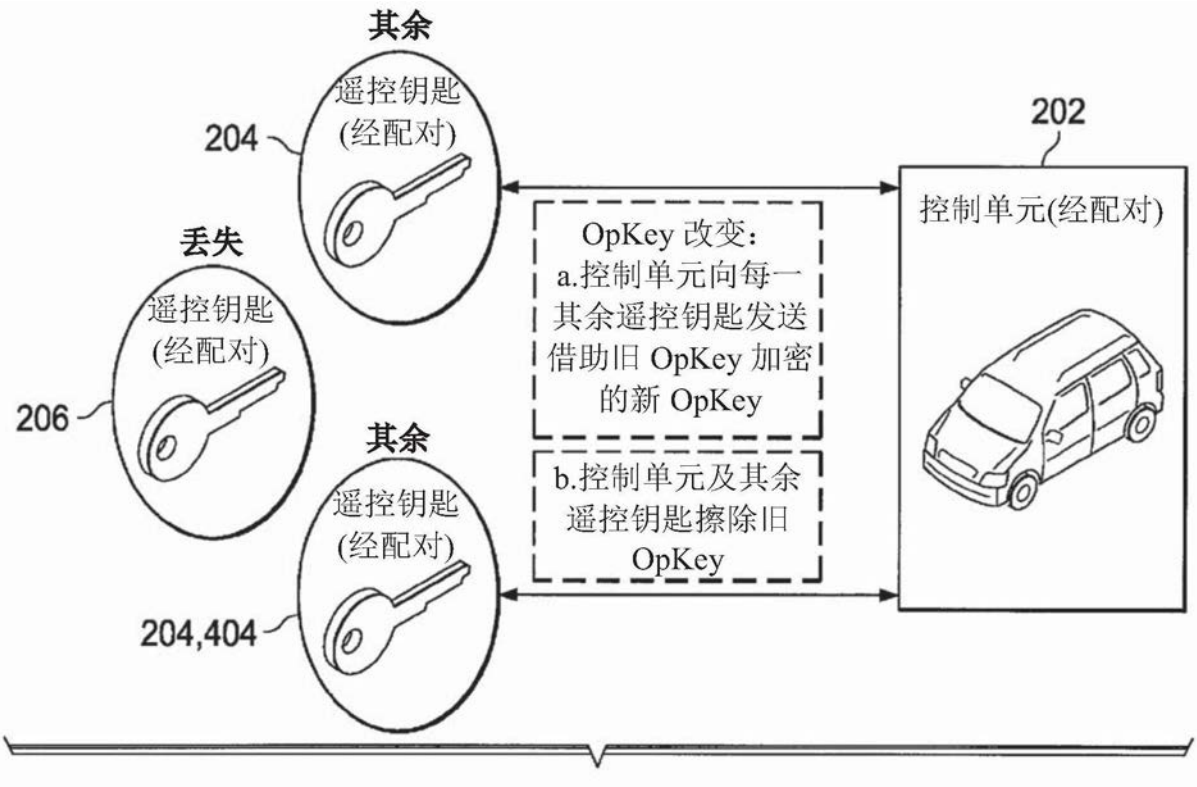

其余
遥控钥匙
(经配对)
204
202
控制单元(经配对)
丢失
遥控钥匙
(经配对)
206
OpKey 改变：
a.控制单元向每一
其余遥控钥匙发送
借助旧 OpKey 加密
的新 OpKey
其余
遥控钥匙
(经配对)
b.控制单元及其余
遥控钥匙擦除旧
OpKey
204,404

图 8

图8

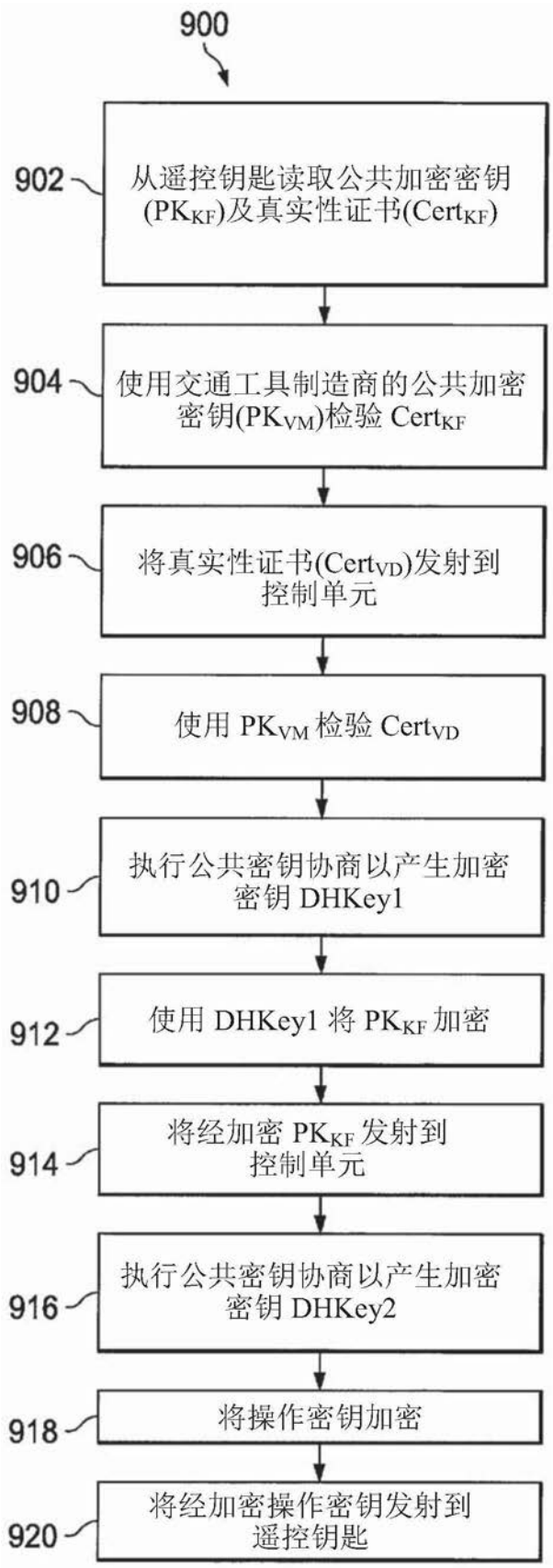

900
902
从遥控钥匙读取公共加密密钥(PK_{KF})及真实性证书($Cert_{KF}$)
904
使用交通工具制造商的公共加密密钥(PK_{VM})检验 $Cert_{KF}$
906
将真实性证书($Cert_{VD}$)发射到控制单元
908
使用 PK_{VM} 检验 $Cert_{VD}$
910
执行公共密钥协商以产生加密密钥 DHKey1
912
使用 DHKey1 将 PK_{KF} 加密
914
将经加密 PK_{KF} 发射到控制单元
916
执行公共密钥协商以产生加密密钥 DHKey2
918
将操作密钥加密
920
将经加密操作密钥发射到遥控钥匙

图9