(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 104412537 B
(45)授权公告日 2019.01.18

(21)申请号 201380035187.2

(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 104412537 A

(43)申请公布日 2015.03.11

(30)优先权数据
61/672,474 2012.07.17 US
61/672,463 2012.07.17 US
13/942,381 2013.07.15 US

(85)PCT国际申请进入国家阶段日
2014.12.30

(86)PCT国际申请的申请数据
PCT/US2013/050735 2013.07.16

(87)PCT国际申请的公布数据
WO2014/014945 EN 2014.01.23

(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 9/00(2006.01)
H04L 9/32(2006.01)

(56)对比文件
US 2010199095 A1,2010.08.05,
US 2012159170 A1,2012.06.21,
CN 101855861 A,2010.10.06,
EP 2003813 A1,2008.12.17,
CN 101135905 A,2008.03.05,
US 2007200671 A1,2007.08.30,

审查员 陈馨

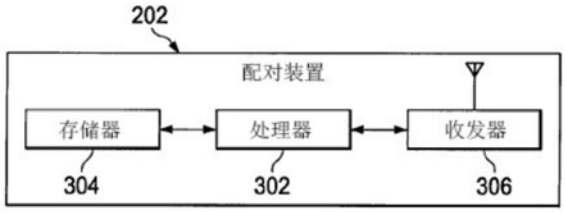
权利要求书2页 说明书4页 附图5页

(54)发明名称

用于配对的方法、配对装置以及遥控钥匙

(57)摘要

本发明涉及一种遥控钥匙-控制单元配对装置(202),其包含:收发器(306),其经配置以发射及接收信号;存储器(304),其经配置以存储遥控钥匙标识KFID及控制单元标识CUID;及处理器(302),其耦合到所述收发器及存储器。所述处理器经配置以基于所述KFID使用标识ID验证密钥协商协议验证所述遥控钥匙且将经加密CUID发射到所述遥控钥匙。



CN 104412537 B

1.一种用于将遥控钥匙与交通工具配对的方法,其包括:

由配对装置及所述遥控钥匙基于遥控钥匙标识KFID执行标识ID验证密钥协商协议以彼此验证且产生第一加密密钥;

由所述配对装置借助所述第一加密密钥将控制单元标识CUID加密;

由所述配对装置将经加密的CUID发射到遥控钥匙;

由所述遥控钥匙及控制单元基于所述CUID执行ID验证密钥协商协议以彼此验证且产生第二加密密钥;

由所述控制单元借助所述第二加密密钥将操作密钥加密;及

由所述控制单元将经加密的操作密钥发射到所述遥控钥匙。

2.根据权利要求1所述的方法,其中:

在执行所述ID验证密钥协商协议之前,所述方法进一步包括将所述CUID插入到所述控制单元的存储装置中;及将所述CUID发射到交通工具经销商。

3.根据权利要求2所述的方法,其进一步包括在将所述CUID发射到所述交通工具经销商之后,将所述KFID插入到所述遥控钥匙中。

4.根据权利要求3所述的方法,其进一步包括在将所述KFID插入到所述遥控钥匙之后,读取所述遥控钥匙的所述KFID。

5.一种遥控钥匙-控制单元配对装置,其包括:

收发器,其发射及接收信号;

存储器,其存储遥控钥匙标识KFID及控制单元标识CUID;及

处理器,其耦合到所述收发器及存储器,以:

基于所述KFID执行标识ID验证密钥协商协议以产生在所述遥控钥匙与所述配对装置之间共享的共用秘密加密密钥;

通过使用所述共用秘密加密密钥产生加密CUID来验证所述遥控钥匙,所述共用秘密加密密钥由所述标识ID验证密钥协商协议产生;以及

将经加密的CUID发射到所述遥控钥匙。

6.根据权利要求5所述的装置,其中所述ID验证密钥协商协议是基于椭圆曲线密码术。

7.根据权利要求5所述的装置,其中所述ID验证密钥协商协议是基于迪菲-赫尔曼密钥协商协议。

8.根据权利要求5所述的装置,其中所述KFID及所述CUID为八字符十六进制字。

9.根据权利要求5所述的装置,其中所述KFID用作用于验证的口令。

10.根据权利要求5所述的装置,其中所述KFID由所述处理器经由所述收发器从所述遥控钥匙接收。

11.一种遥控钥匙,其包括:

收发器,其接收及发送信号;

存储器,其存储遥控钥匙标识KFID;及

处理器,其耦合到所述收发器及存储器,以:

连同配对装置一起基于所述KFID执行标识ID验证密钥协商协议以验证配对装置且产生仅被所述处理器及所述配对装置知晓的共用秘密加密密钥;

从所述配对装置接收由所述配对装置借助所述共用秘密加密密钥加密的控制单元标

识CUID；

连同与所述CUID相关联的控制单元一起基于所述CUID执行ID验证密钥协商协议以验证所述控制单元且产生仅被所述处理器及所述控制单元知晓的第二共用秘密加密密钥；及

从所述控制单元接收由所述控制单元借助所述第二共用秘密加密密钥加密的操作密钥。

12.根据权利要求11所述的遥控钥匙，其中所述ID验证密钥协商协议是基于椭圆曲线密码术。

13.根据权利要求11所述的遥控钥匙，其中所述KFID与所述CUID验证密钥协商协议是基于迪菲-赫尔曼密钥协商协议。

14.根据权利要求11所述的遥控钥匙，其中所述处理器用以借助所述第二共用秘密加密密钥将所述操作密钥解密。

15.根据权利要求11所述的遥控钥匙，其中所述KFID及所述CUID为八字符十六进制字。

16.根据权利要求11所述的遥控钥匙，其中经加密的操作密钥是无线地接收的。

17.根据权利要求11所述的遥控钥匙，其中处理器使用所述共用秘密加密密钥将经加密的CUID解密。

用于配对的方法、配对装置以及遥控钥匙

背景技术

[0001] 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需要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

[0002] 上文所述的问题大部分通过遥控钥匙-控制单元配对装置解决，所述配对装置包含：收发器，其用以发射及接收信号；存储器，其用以存储遥控钥匙标识KFID及控制单元标识CUID；及处理器，其耦合到所述收发器及存储器。所述处理器用以基于所述KFID使用标识(ID)验证密钥协商协议验证所述遥控钥匙且将经加密CUID发射到所述遥控钥匙。

[0003] 对所述问题的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，其用以存储遥控钥匙标识(KFID)；及处理器，其耦合到所述收发器及存储器。所述处理器用以连同配对装置一起基于所述KFID执行标识(ID)验证密钥协商协议以验证所述配对装置且产生仅被所述处理器及所述配对装置知晓的共用秘密加密密钥。所述处理器还用以从所述配对装置接收由所述配对装置借助所述共用秘密加密密钥加密的控制单元标识CUID，用以连同与所述CUID相关联的控制单元一起基于所述CUID执行(ID)验证密钥协商协议以验证所述控制单元且产生仅被所述处理器及所述控制单元知晓的第二共用秘密加密密钥，且用以从所述控制单元接收由所述控制单元借助所述第二共用秘密加密密钥加密的操作密钥。

[0004] 且另一解决方案可为一种用于将遥控钥匙与交通工具配对的方法，其包含：由配对装置及遥控钥匙基于KFID执行(ID)验证密钥协商协议以彼此验证且产生加密密钥DHKey1；由所述配对装置借助DHKey1将控制单元标识(CUID)加密；由所述配对装置将所述经加密CUID发射到遥控钥匙；由所述遥控钥匙及控制单元基于所述CUID执行(ID)验证密钥协商协议以彼此验证且产生加密密钥DHKey2；由所述控制单元借助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

[0005] 图1图解说明用于根据本文中所论述的各种实例的基于标识(ID)的验证配对方法的实例性调节过程。

[0006] 图2图解说明使用基于ID的验证且根据本文中所论述的各种实例的遥控钥匙与控制单元的实例性初始配对过程。

[0007] 图3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。

[0008] 图4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。

[0009] 图5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。

[0010] 图6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。

[0011] 图7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。

[0012] 图8是根据本文中所论述的各种实例的用于基于ID的验证的实例性方法的流程图。

具体实施方式

[0013] 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。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,此过程可能需要制造商开发昂贵且专用的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经销商时,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。

[0014] 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。

[0015] 本文中揭示的是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经销商的输送且可减少交通工具制造商的IT需求。一种用以实现遥控钥匙与控制单元的配对的方法可涉及标识(ID)验证密钥协商协议,其中ID充当用于验证目的的口令。借助基于ID的验证方法,遥控钥匙及控制单元两者均可具有其自身的唯一相关联ID。所述ID可接着在密钥协商协议中使用来产生可用于在装置之间传递信息的共用秘密加密密钥,因此将遥控钥匙与控制单元配对。配对装置可首先使用遥控钥匙的ID产生与遥控钥匙的秘密密钥。所述秘密密钥可接着由配对装置使用来对控制单元的ID进行加密。经加密控制单元ID可接着发射到遥控钥匙,因此遥控钥匙知晓与哪一控制单元配对。遥控钥匙及控制单元可接着使用控制单元ID来产生仅被其知晓的第二秘密密钥。第二秘密密钥可接着由控制单元使用来对操作密钥进行加密,操作密钥将发射到遥控钥匙以完成配对过程。

[0016] 其中ID充当用于验证的口令的ID验证密钥协商协议可基于椭圆曲线密码术(ECC),例如椭圆曲线迪菲-赫尔曼(Diffie-Hellman)密钥协商协议。

[0017] 基于ID的技术的可能优点为其可不需要成本高的公共密钥基础结构及证书授权机构。

[0018] 图1图解说明用于根据本文中所论述的各种实例的基于标识(ID)的验证配对方法的实例性调节过程100。调节过程100可使遥控钥匙及CU准备好,以便促进所述两者的配对。调节过程可涉及交通工具经销商112、交通工具制造商110、遥控钥匙106及CU104。替代地,交通工具经销商112在调节过程100中的部分可在将遥控钥匙与CU配对时发生且不必如图1

中所展示执行。调节过程100可涉及将唯一ID插入到CU 104(CUID)及遥控钥匙106(KFID)中。CU 104的唯一ID可被保秘且可由交通工具制造商110或对交通工具制造商110的CU 104供应商插入到CU 104中。举例来说，遥控钥匙及CU两者的唯一ID可为八字符十六进制字。替代地，ID可基于允许大量排列以避免所使用的ID内的冗余的系统。ID可经选择使得假冒者/对手不能预测经销商112可在接下来的配对中使用哪一遥控钥匙106(及其相关联KFID)。八字符十六进制ID将产生约40亿种可能性。

[0019] 交通工具制造商110可将相关联CU 104的CUID发送到交通工具经销商112，交通工具经销商112接收包含那些CU 104的交通工具。CUID到经销商112的传送应经执行使得CUID被保秘。经拦截CUID可允许产生假冒遥控钥匙，所述假冒遥控钥匙可与CU配对而无需经销商112的帮助，此可能导致盗窃。

[0020] 遥控钥匙106可具有其唯一ID(KFID)，所述KFID不必保密且可从遥控钥匙106读取，由遥控钥匙制造商102、遥控钥匙组装者或交通工具制造商110插入。

[0021] 图2图解说明使用基于ID的验证且根据本文中所论述的各种实例的遥控钥匙与控制单元的实例性初始配对过程200。初始配对200可涉及配对装置202(在经销商112处)、遥控钥匙106及CU 104。类似于上文所论述的基于证书的验证方法，配对装置202可通过将标识信息安全地传送到所述组件中的一者以用来连接到其它组件而促进遥控钥匙106与CU 104的配对。

[0022] 配对过程200可在步骤1a处以经销商112从库存中的许多遥控钥匙中选择一个遥控钥匙106开始。在选择时且在整个配对过程中，遥控钥匙106的KFID应被保密。步骤1b，经销商112可接着将相关联遥控钥匙106的KFID及CU 104的CUID秘密地输入到配对装置202中。

[0023] 配对装置202可接着建立与遥控钥匙106的通信，步骤2a。使用KFID，配对装置及遥控钥匙106可接着执行ID验证密钥协商协议，其中ID充当用于验证目的的口令。ID验证密钥协商协议可执行两个功能：使两个组件彼此进行验证及产生所述两个组件可使用来在彼此间发射经加密消息的共用秘密密钥。因此，当配对装置202及遥控钥匙使用KFID执行ID验证密钥协商协议时，其彼此验证且其将产生共用秘密密钥DHKey1来用于与彼此的安全通信。在步骤2b处，配对装置202可使用DHKey1将CUID加密且将经加密CUID发射到遥控钥匙106。

[0024] 遥控钥匙106可能够将消息解密以获得CUID，CUID可接着用于建立与和所接收CUID相关联的CU 104的通信。在步骤3a处，遥控钥匙106及CU 104可接着使用CUID执行基于ID的加密验证(类似于上文)以既彼此验证又产生共用秘密密钥DHKey2。在步骤3b处，CU 104可接着使用DHKey2来将OpKey加密以发射到遥控钥匙106。另外或替代地，遥控钥匙106可在与CU 104的初始配对之后擦除CUID。

[0025] 图3、4及5分别是根据本文中所论述的各种实例的实例性配对装置202、遥控钥匙106及CU 104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(302、402、502)，存储器(304、404、504)及收发器(306、406、506)。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。

[0026] 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202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202的存储器304中。存储器可为非易失性存储装置，例如快闪存储器或EEPROM。

[0027] 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。收发器可由装置使用来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。

[0028] 图6图解说明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6中所描绘的正常操作展示遥控钥匙106与CU 104在通过过程200(基于ID)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验证的质询-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。

[0029] 图7图解说明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 104可在遥控钥匙106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106接入CU 104。CU 104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106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202。在接收到外部信号后，CU 104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106。在接收到新OpKey之后，可由所有CU 104及其余遥控钥匙106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。

[0030] 图8是根据本文中所论述的各种实例的用于基于ID的验证的实例性方法800的流程图。方法800可为关于图5所描述的初始配对过程200的一个实施方案。方法800在步骤802处以配对装置202及遥控钥匙106执行KFID验证密钥协商协议以彼此验证且产生加密密钥DHKey1开始。步骤804借助以下操作继续方法800：在配对装置202在步骤806处以将经加密CUID发射到遥控钥匙106而继续之前，所述配对装置借助DHKey1将CU 104的CUID加密。

[0031] 方法800在步骤808处以遥控钥匙106及CU 104执行CUID验证密钥协商协议以彼此验证且产生加密密钥DHKey2继续。方法800接着以步骤810及812结束，其中CU 104借助DHKey2将OpKey加密且将经加密OpKey发射到遥控钥匙106。在OpKey已与遥控钥匙106共享之后，CU 104与遥控钥匙106可视为经配对的。

[0032] 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为可能的。

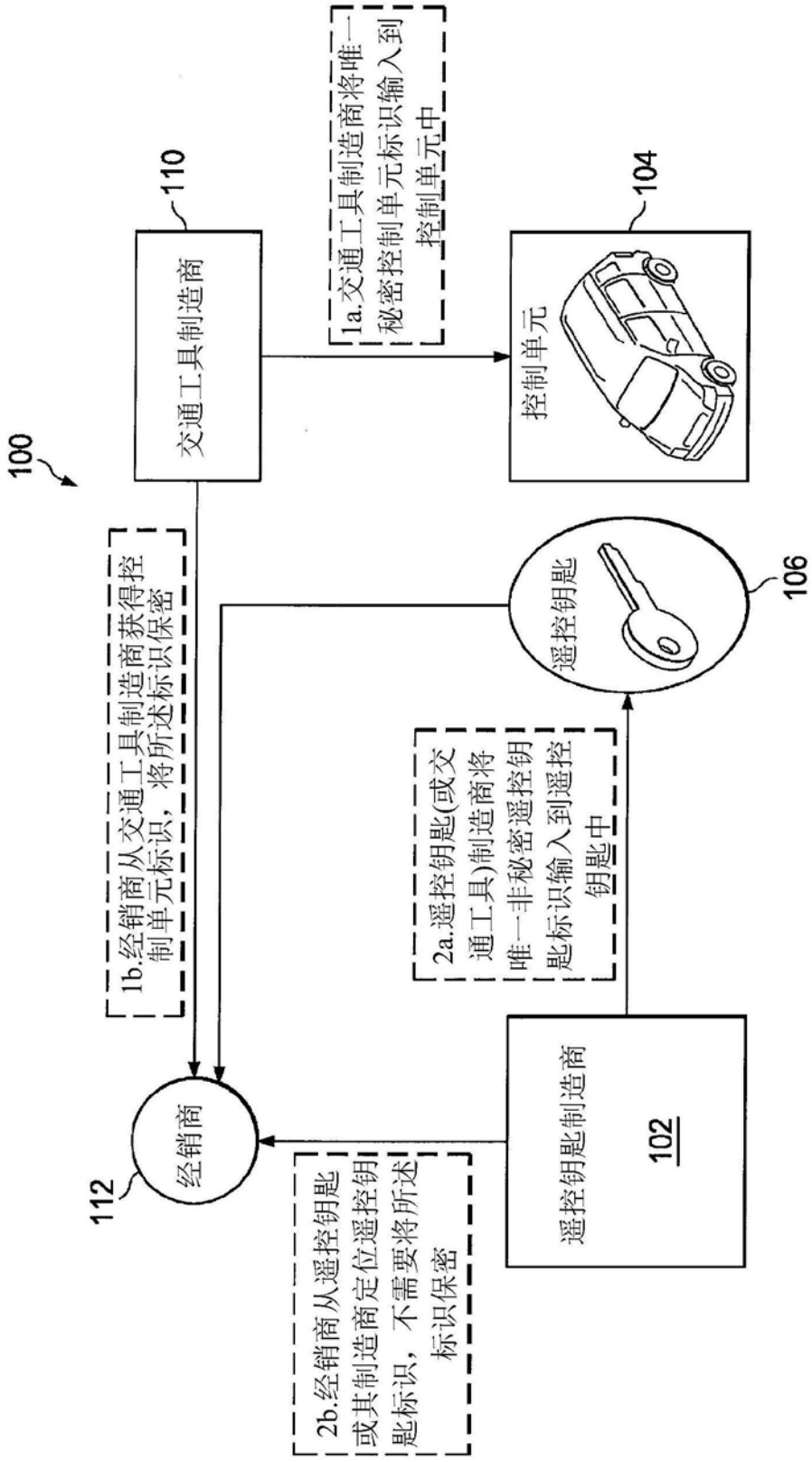

100
交通工具制造商
110
1a.交通工具制造商将唯一秘密控制单元标识输入到控制单元中
控制单元
104
1b.经销商从交通工具制造商获得控制单元标识，将所述标识保密
遥控钥匙
106
2a.遥控钥匙(或交通工具)制造商将唯一非秘密遥控钥匙标识输入到遥控钥匙中
经销商
112
2b.经销商从遥控钥匙或其制造商定位遥控钥匙标识，不需要将所述标识保密
遥控钥匙制造商
102

图1

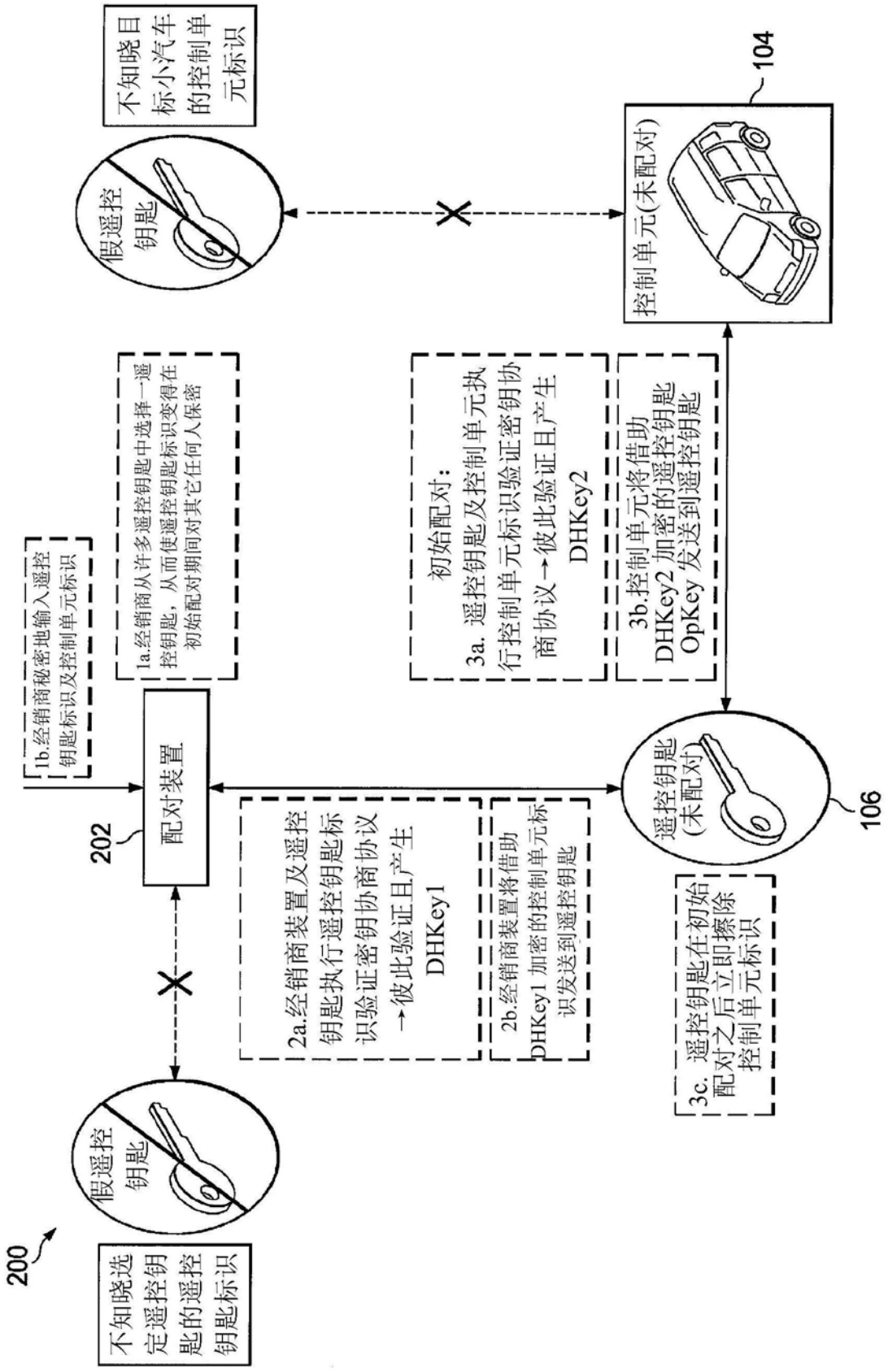

200
不知晓选定遥控钥匙的遥控钥匙标识
假遥控钥匙
不知晓目标小汽车的控制单元标识
假遥控钥匙
104
控制单元(未配对)
1a.经销商从许多遥控钥匙中选择一遥控钥匙，从而使遥控钥匙标识变得在初始配对期间对其它任何人保密
1b.经销商秘密地输入遥控钥匙标识及控制单元标识
202
配对装置
初始配对：
3a. 遥控钥匙及控制单元执行控制单元标识验证密钥协商协议→彼此验证且产生DHKey2
3b.控制单元将借助DHKey2 加密的遥控钥匙OpKey 发送到遥控钥匙
2a.经销商装置及遥控钥匙执行遥控钥匙标识验证密钥协商协议→彼此验证且产生DHKey1
2b.经销商装置将借助DHKey1 加密的控制单元标识发送到遥控钥匙
遥控钥匙(未配对)
106
3c. 遥控钥匙在初始配对之后立即擦除控制单元标识

图2

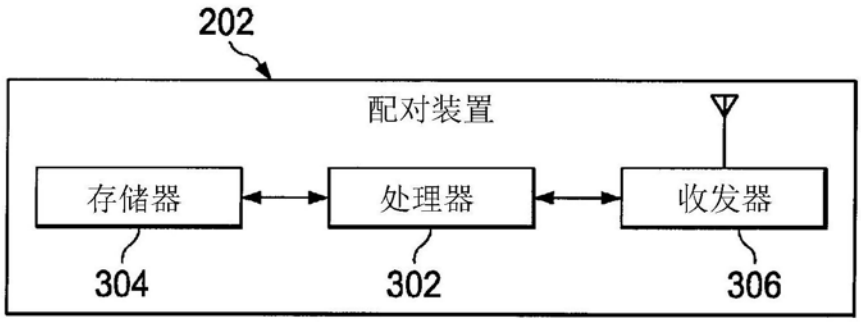

202
配对装置
存储器
处理器
收发器
304
302
306

图3

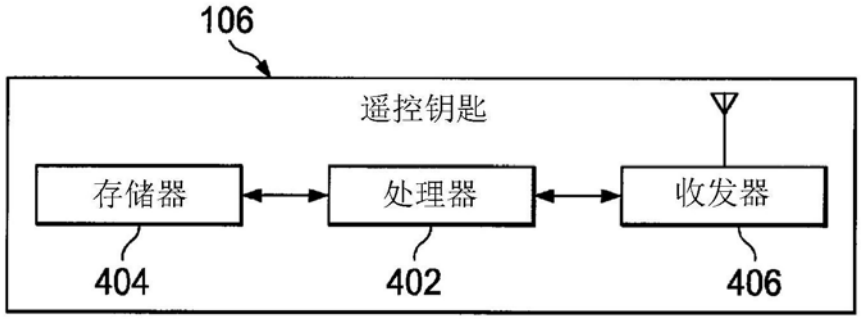

106
遥控钥匙
存储器
处理器
收发器
404
402
406

图4

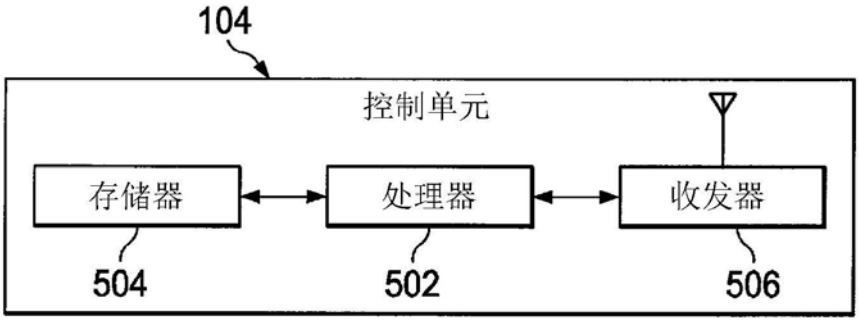

104
控制单元
存储器
处理器
收发器
504
502
506

图5

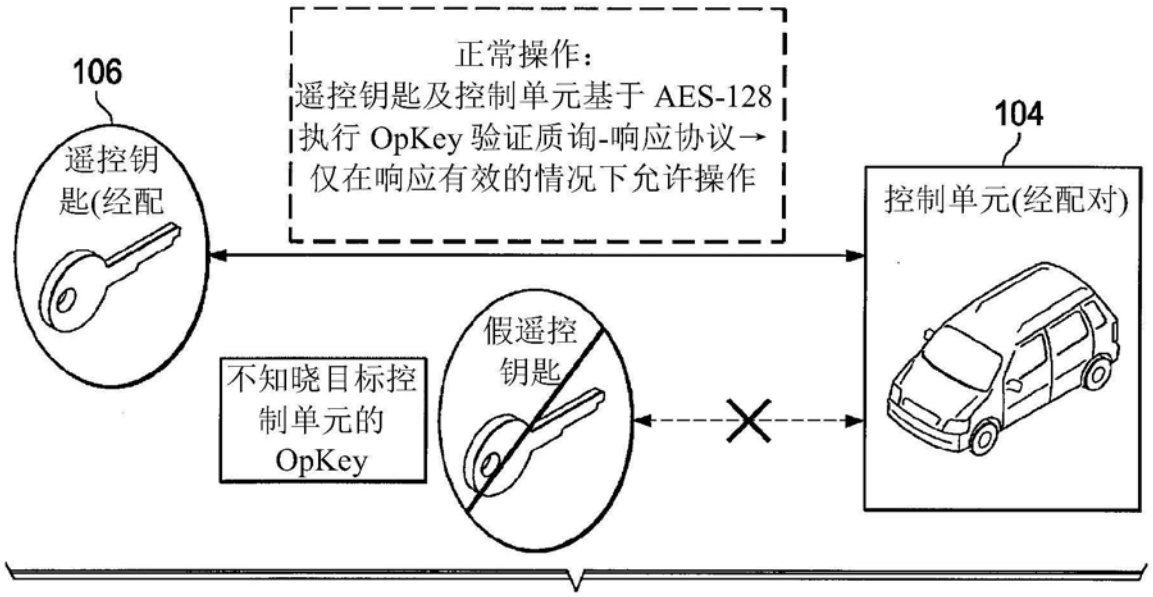

106
遥控钥匙(经配
正常操作：
遥控钥匙及控制单元基于 AES-128
执行 OpKey 验证质询-响应协议→
仅在响应有效的情况下允许操作
104
控制单元(经配对)
不知晓目标控制单元的 OpKey
假遥控钥匙

图6

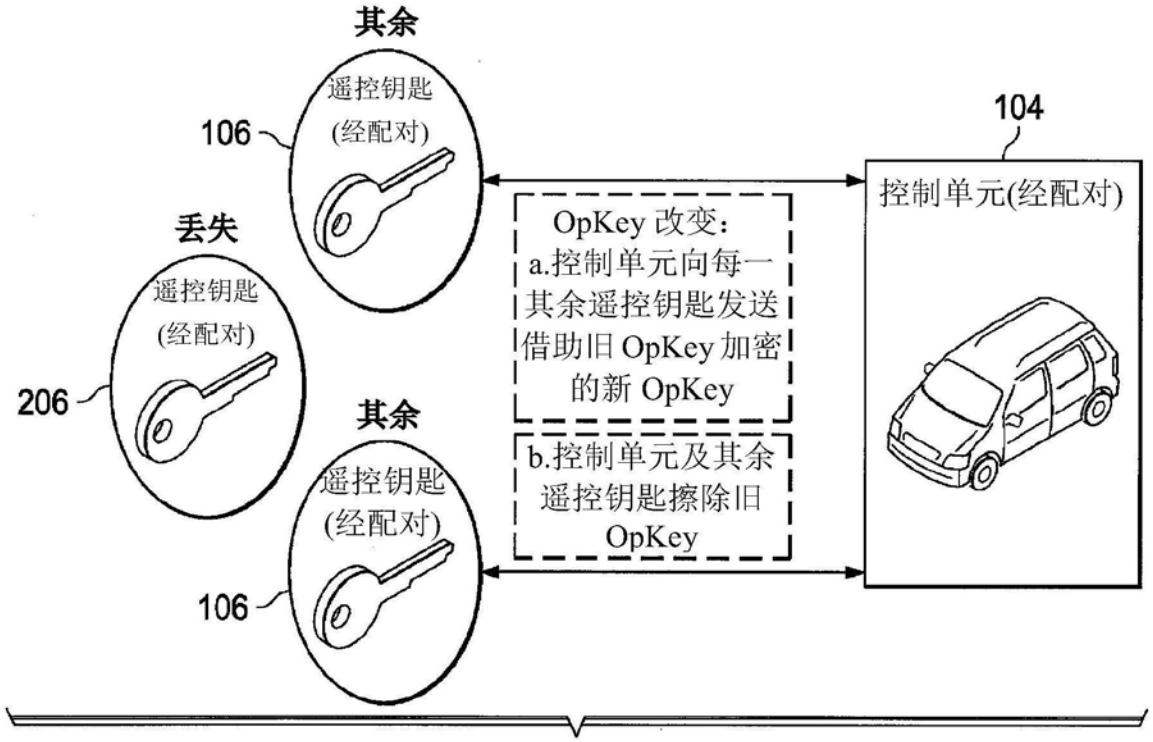

其余
遥控钥匙(经配对)
106
104
控制单元(经配对)
丢失
遥控钥匙(经配对)
206
OpKey 改变：
a.控制单元向每一其余遥控钥匙发送借助旧 OpKey 加密的新 OpKey
其余
遥控钥匙(经配对)
b.控制单元及其余遥控钥匙擦除旧 OpKey
106

图7

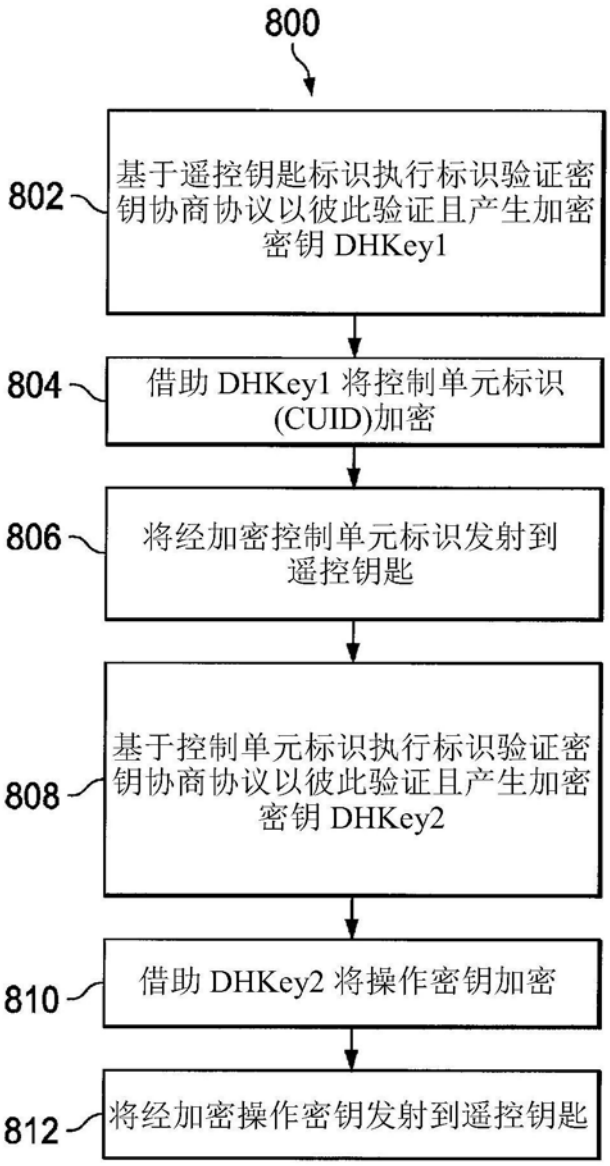

800
802
基于遥控钥匙标识执行标识验证密钥协商协议以彼此验证且产生加密密钥 DHKey1
804
借助 DHKey1 将控制单元标识(CUID)加密
806
将经加密控制单元标识发射到遥控钥匙
808
基于控制单元标识执行标识验证密钥协商协议以彼此验证且产生加密密钥 DHKey2
810
借助 DHKey2 将操作密钥加密
812
将经加密操作密钥发射到遥控钥匙

图8