(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 107925568 A
(43)申请公布日 2018.04.17

(21)申请号 201680045405.4

(22)申请日 2016.08.04

(30)优先权数据
2015-155376 2015.08.05 JP
2015-239428 2015.12.08 JP

(85)PCT国际申请进入国家阶段日
2018.02.01

(86)PCT国际申请的申请数据
PCT/JP2016/072926 2016.08.04

(87)PCT国际申请的公布数据
WO2017/022821 JA 2017.02.09

(71)申请人 KDDI株式会社
地址 日本东京都

(72)发明人 竹森敬祐 川端秀明 小林靖明

(74)专利代理机构 隆天知识产权代理有限公司 72003
代理人 向勇

(51)Int.Cl.
H04L 9/08(2006.01)
G06F 21/44(2006.01)
G06F 21/45(2006.01)
H04L 9/14(2006.01)

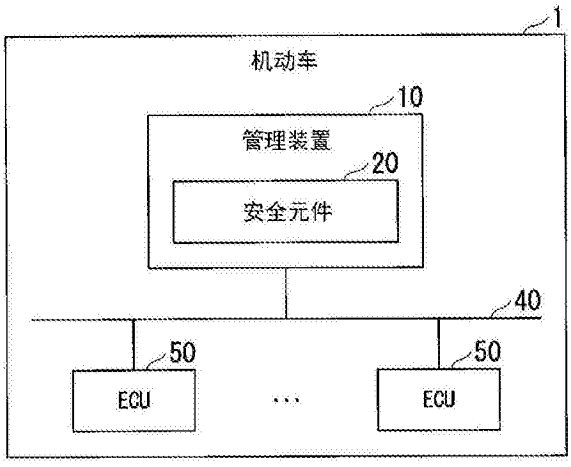
权利要求书5页 说明书24页 附图15页

(54)发明名称

管理装置、管理系统、密钥生成装置、密钥生成系统、密钥管理系统、车辆、管理方法、密钥生成方法以及计算机程序

(57)摘要

机动车具有的管理装置具有：主密钥存储部，存储与和ECU标识符一起用于生成在ECU中保存的初始密钥的主密钥相同的主密钥；通信部，与ECU进行通信；密钥生成部，使用在主密钥存储部中存储的主密钥和通过通信部从ECU接收到的ECU标识符，来生成ECU的初始密钥；以及初始密钥存储部，将由密钥生成部生成的ECU的初始密钥与ECU标识符关联地存储。



CN 107925568 A

1.一种管理装置,在车辆具有该管理装置,其中,所述管理装置具有:

主密钥存储部,存储主密钥,该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同,所述初始密钥被保存在所述车辆具有的所述车载计算机中;

通信部,与所述车载计算机进行通信;

密钥生成部,使用在所述主密钥存储部中存储的主密钥和通过所述通信部从所述车载计算机接收到的所述车载计算机的标识符,来生成所述车载计算机的初始密钥;以及

初始密钥存储部,将由所述密钥生成部生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

2.一种管理系统,具有管理装置和管理服务器装置,在车辆具有该管理装置,该管理服务器装置经由无线通信网络与所述管理装置进行通信,其中,

所述管理服务器装置具有:

存储部,存储主密钥,该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同,所述初始密钥被保存在所述车辆具有的所述车载计算机中;

密钥生成部,使用在所述存储部中存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符,来生成所述车载计算机的初始密钥;以及

通信部,将由所述密钥生成部生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理装置,

所述管理装置具有:

无线通信部,将所述车载计算机的标识符经由所述无线通信网络发送给所述管理服务器装置,并从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组;以及

密钥存储部,存储通过所述无线通信部从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

3.一种管理装置,在车辆具有该管理装置,其中,所述管理装置具有:

无线通信部,经由无线通信网络向管理服务器装置发送车载计算机的标识符,并从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组,所述车载计算机的标识符与主密钥一起用于生成初始密钥,所述初始密钥被保存在所述车辆具有的所述车载计算机中,所述管理服务器装置具有与所述主密钥相同的主密钥;以及

密钥存储部,存储通过所述无线通信部从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

4.一种密钥生成装置,在车辆具有该密钥生成装置,其中,

所述密钥生成装置具有密钥存储部,该密钥存储部存储多个主密钥,所述多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同,所述初始密钥被保存在所述车辆具有的所述车载计算机中,

所述密钥生成装置使用在所述密钥存储部中存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符,来生成所述车载计算机的初始密钥。

5.一种密钥管理系统,其中,具有:

权利要求4所述的密钥生成装置;以及

密钥存储部，将由所述密钥生成装置生成的车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

6.一种密钥生成系统，在车辆具有该密钥生成系统，其中，

所述密钥生成系统具有第一值生成装置和初始密钥生成装置，

所述第一值生成装置具有第一密钥存储部，该第一密钥存储部存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中，

所述第一值生成装置使用在所述第一密钥存储部中存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值，

所述初始密钥生成装置具有第二密钥存储部，该第二密钥存储部存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中，

所述初始密钥生成装置使用在所述第二密钥存储部中存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

7.根据权利要求6所述的密钥生成系统，其中，

所述第一值生成装置和所述初始密钥生成装置分别由标准不同的安全元件构成。

8.根据权利要求7所述的密钥生成系统，其中，

所述第一值生成装置和所述初始密钥生成装置分别由防篡改技术的标准不同的安全元件构成。

9.一种密钥管理系统，其中，具有：

权利要求6至8中的任一项所述的密钥生成系统；以及

密钥存储部，将由所述密钥生成系统生成的车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

10.一种车辆，具有权利要求1或3所述的管理装置。

11.一种车辆，具有权利要求4所述的密钥生成装置或权利要求6所述的密钥生成系统。

12.一种管理方法，其中，包括：

主密钥存储步骤，在车辆具有的管理装置存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；

通信步骤，所述管理装置从所述车载计算机接收所述车载计算机的标识符；

密钥生成步骤，所述管理装置使用通过所述主密钥存储步骤存储的主密钥和通过所述通信步骤从所述车载计算机接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及

初始密钥存储步骤，所述管理装置将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

13.一种管理方法，为管理系统的管理方法，所述管理系统具有管理装置和管理服务器

装置，在车辆具有该管理装置，该管理服务器装置经由无线通信网络与所述管理装置进行通信，其中，所述管理方法包括：

存储步骤，所述管理服务器装置存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；

密钥生成步骤，所述管理服务器装置使用通过所述存储步骤存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及

通信步骤，所述管理服务器装置将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理装置，

发送步骤，所述管理装置经由所述无线通信网络向所述管理服务器装置发送所述车载计算机的标识符；

接收步骤，所述管理装置从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组；以及

密钥存储步骤，所述管理装置存储通过所述接收步骤从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

14.一种密钥生成方法，其中，包括：

主密钥存储步骤，在车辆具有的密钥生成装置存储多个主密钥，所述多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及

密钥生成步骤，所述密钥生成装置使用通过所述主密钥存储步骤存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成所述车载计算机的初始密钥。

15.一种密钥生成方法，其中，包括：

第一主密钥存储步骤，在车辆具有的第一值生成装置存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中；

第一值生成步骤，所述第一值生成装置使用通过所述第一主密钥存储步骤存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值；

第二主密钥存储步骤，在所述车辆具有的初始密钥生成装置存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中；以及

初始密钥生成步骤，所述初始密钥生成装置使用通过所述第二主密钥存储步骤存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

16.一种计算机程序，所述计算机程序用于使在车辆具有的管理装置的计算机执行：

主密钥存储步骤，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；

通信步骤，从所述车载计算机接收所述车载计算机的标识符；

密钥生成步骤，使用通过所述主密钥存储步骤存储的主密钥和通过所述通信步骤从所述车载计算机接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及

初始密钥存储步骤，将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

17.一种计算机程序，所述计算机程序用于使经由无线通信网络与在车辆具有的管理装置进行通信的管理服务器装置的计算机执行：

存储步骤，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；

密钥生成步骤，使用通过所述存储步骤存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及

通信步骤，将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理装置。

18.一种计算机程序，所述计算机程序用于使在车辆具有的管理装置的计算机执行：

发送步骤，经由无线通信网络向管理服务器装置发送车载计算机的标识符，所述车载计算机的标识符与主密钥一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中，所述管理服务器装置具有与所述主密钥相同的主密钥；

接收步骤，从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组；以及

密钥存储步骤，存储通过所述接收步骤从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

19.一种计算机程序，所述计算机程序用于使在车辆具有的密钥生成装置的计算机执行：

主密钥存储步骤，存储多个主密钥，该多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及

密钥生成步骤，使用通过所述主密钥存储步骤存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成所述车载计算机的初始密钥。

20.一种计算机程序，其中，

所述计算机程序用于使在车辆具有的第一值生成装置的计算机执行：

第一主密钥存储步骤，存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及

第一值生成步骤，使用通过所述第一主密钥存储步骤存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值，

所述计算机程序用于使在所述车辆具有的初始密钥生成装置的计算机执行：

第二主密钥存储步骤，存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥

相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中；以及

初始密钥生成步骤，使用通过所述第二主密钥存储步骤存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

管理装置、管理系统、密钥生成装置、密钥生成系统、密钥管理系统、车辆、管理方法、密钥生成方法以及计算机程序

技术领域

[0001] 本发明涉及管理装置、管理系统、密钥生成装置、密钥生成系统、密钥管理系统、车辆、管理方法、密钥生成方法以及计算机程序。

[0002] 本申请基于2015年8月5日在日本申请的特愿2015-155376号及2015年12月8日在日本申请的特愿2015-239428号而要求优先权，并在本文援引其内容。

背景技术

[0003] 近年来，机动车具有ECU(Electronic Control Unit;电子控制单元)，通过ECU来实现发动机控制等功能。ECU是计算机的一种，通过计算机程序来实现期望的功能。关于已经被使用的机动车，ECU的计算机程序的更新通常在机动车的检查时、定期检查时等在一般的机动车维修厂进行。

[0004] 以往，ECU的计算机程序的更新中，操作者将专用于维护的诊断终端连接到被称为机动车的OBD(On-board Diagnostics;车载诊断)端口的诊断端口，从该诊断终端进行更新程序的安装以及数据的设定变更等。关于此，例如在非专利文献1、2中记载了车载控制系统的安全性。

[0005] 现有技术文献

[0006] 非专利文献

[0007] 非专利文献1:C.Miller,C.Valasek,“Adventures in Automotive Networks and Control Units(汽车网络和控制单元的冒险)”,DEF CON 21,2013年8月

[0008] 非专利文献2:高田广章，松本勉，“車載组込みシステムの情報セキュリティ強化に関する提言(关于加强车载嵌入式系统信息安全的建议)”，2013年9月，互联网＜URL:https://www.ipa.go.jp/files/000034668.pdf＞

[0009] 非专利文献3:Trusted Computing Group(可信计算组)，互联网＜URL:http://www.trustedcomputinggroup.org/＞

发明内容

[0010] 发明要解决的问题

[0011] 上述的非专利文献1、2中未记载有关实现车载控制系统的安全性的提高的方法。因此，期望提高关于在机动车等车辆具有的ECU等车载计算机所使用的计算机程序等的数据应用的可靠性。

[0012] 例如，考虑在ECU启动后，通过使用ECU保存的密钥而相互认证数据的交换对象，从而提高车载计算机系统的防御能力。此外，例如，考虑使用ECU保存的密钥来验证在ECU间交换的数据的合法性。此外，例如，考虑通过对ECU所使用的计算机程序等的数据附加电子署名并分配给机动车的管理装置，使用管理装置保存的密钥来验证被分配的数据的电子署名，从而检查ECU所使用的计算机程序等的数据。此处，如何实现机动车所保存的密钥的管

理、更新是一个关键的安保问题。

[0013] 本发明是鉴于这种情况而提出的，其课题在于，提供能够有助于机动车等车辆中保存的密钥的管理、更新的管理装置、管理系统、密钥生成装置、密钥生成系统、密钥管理系统、车辆、管理方法、密钥生成方法以及计算机程序。

[0014] 解决问题的技术方案

[0015] (1)本发明的一个方式的管理装置是在车辆具有的管理装置，所述管理装置具有：主密钥存储部，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；通信部，与所述车载计算机进行通信；密钥生成部，使用在所述主密钥存储部中存储的主密钥和通过所述通信部从所述车载计算机接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及初始密钥存储部，将由所述密钥生成部生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

[0016] (2)本发明的一个方式的管理系统是具有管理装置和管理服务器装置的管理系统，在车辆具有该管理装置，该管理服务器装置经由无线通信网络与所述管理装置进行通信，其中，所述管理服务器装置具有：存储部，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；密钥生成部，使用在所述存储部中存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及通信部，将由所述密钥生成部生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理装置，所述管理装置具有：无线通信部，将所述车载计算机的标识符经由所述无线通信网络发送给所述管理服务器装置，并从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组；以及密钥存储部，存储通过所述无线通信部从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

[0017] (3)本发明的一个方式的管理装置是在车辆具有的管理装置，所述管理装置具有：无线通信部，经由无线通信网络向管理服务器装置发送车载计算机的标识符，并从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组，所述车载计算机的标识符与主密钥一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中，所述管理服务器装置具有与所述主密钥相同的主密钥；以及密钥存储部，存储通过所述无线通信部从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

[0018] (4)本发明的一个方式的密钥生成装置是在车辆具有的密钥生成装置，其中，所述密钥生成装置具有密钥存储部，该密钥存储部存储多个主密钥，该多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中，所述密钥生成装置使用在所述密钥存储部中存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成所述车载计算机的初始密钥。

[0019] (5)本发明的一个方式的密钥管理系统具有：上述(4)的密钥生成装置；以及密钥存储部，将由所述密钥生成装置生成的车载计算机的初始密钥与所述车载计算机的标识符

关联地存储。

[0020] (6)本发明的一个方式的密钥生成系统是在车辆具有的密钥生成系统，其中，所述密钥生成系统具有第一值生成装置和初始密钥生成装置，所述第一值生成装置具有第一密钥存储部，该第一密钥存储部存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中，所述第一值生成装置使用在所述第一密钥存储部中存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值，所述初始密钥生成装置具有第二密钥存储部，该第二密钥存储部存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中，所述初始密钥生成装置使用在所述第二密钥存储部中存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

[0021] (7)在本发明的一个方式的上述(6)的密钥生成系统中，所述第一值生成装置和所述初始密钥生成装置可以分别由标准不同的安全元件构成。

[0022] (8)在本发明的一个方式的上述(7)的密钥生成系统中，所述第一值生成装置和所述初始密钥生成装置可以分别由防篡改技术的标准不同的安全元件构成。

[0023] (9)本发明的一个方式的密钥管理系统，具有：上述(6)至(8)的任一项的密钥生成系统；以及密钥存储部，将由所述密钥生成系统生成的车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

[0024] (10)本发明的一个方式的车辆具有上述(1)或(3)的管理装置。

[0025] (11)本发明的一个方式的车辆具有上述(4)的密钥生成装置或上述(6)的密钥生成系统。

[0026] (12)本发明的一个方式的管理方法由在车辆具有的管理装置进行，该管理方法包括：主密钥存储步骤，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；通信步骤，所述管理装置从所述车载计算机接收所述车载计算机的标识符；密钥生成步骤，所述管理装置使用通过所述主密钥存储步骤存储的主密钥和通过所述通信步骤从所述车载计算机接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及初始密钥存储步骤，所述管理装置将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

[0027] (13)本发明的一个方式的管理方法由管理系统进行，所述管理系统具有管理装置和管理服务器装置，在车辆具有该管理装置，该管理服务器装置经由无线通信网络与所述管理装置进行通信，其中，所述管理方法包括：存储步骤，所述管理服务器装置存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；密钥生成步骤，所述管理服务器装置使用通过所述存储步骤存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及通信步骤，所述管理服务器装置将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理

装置，发送步骤，所述管理装置经由所述无线通信网络向所述管理服务器装置发送所述车载计算机的标识符；接收步骤，所述管理装置从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组；以及密钥存储步骤，所述管理装置存储通过所述接收步骤从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

[0028] (14)本发明的一个方式的密钥生成方法由在车辆具有的密钥生成装置进行，该密钥生成方法包括：主密钥存储步骤，存储多个主密钥，该多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及密钥生成步骤，使用通过所述主密钥存储步骤存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成所述车载计算机的初始密钥。

[0029] (15)本发明的一个方式的密钥生成方法由在车辆具有的第一值生成装置及初始密钥生成装置进行，该密钥生成方法包括：第一主密钥存储步骤，所述第一值生成装置存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中；第一值生成步骤，所述第一值生成装置使用通过所述第一主密钥存储步骤存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值；第二主密钥存储步骤，所述初始密钥生成装置存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中；以及初始密钥生成步骤，所述初始密钥生成装置使用通过所述第二主密钥存储步骤存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

[0030] (16)本发明的一个方式的计算机程序，所述计算机程序用于使在车辆具有的管理装置的计算机执行：主密钥存储步骤，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；通信步骤，从所述车载计算机接收所述车载计算机的标识符；密钥生成步骤，使用通过所述主密钥存储步骤存储的主密钥和通过所述通信步骤从所述车载计算机接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及初始密钥存储步骤，将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符关联地存储。

[0031] (17)本发明的一个方式的计算机程序，所述计算机程序用于使经由无线通信网络与在车辆具有的管理装置进行通信的管理服务器装置的计算机执行：存储步骤，存储主密钥，该主密钥与和车载计算机的标识符一起用于生成初始密钥的主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；密钥生成步骤，使用通过所述存储步骤存储的主密钥和经由所述管理装置接收到的所述车载计算机的标识符，来生成所述车载计算机的初始密钥；以及通信步骤，将通过所述密钥生成步骤生成的所述车载计算机的初始密钥与所述车载计算机的标识符一起发送给所述管理装置。

[0032] (18)本发明的一个方式的计算机程序，所述计算机程序用于使在车辆具有的管理装置的计算机执行：发送步骤，经由无线通信网络向管理服务器装置发送车载计算机的标

识符，所述车载计算机的标识符与主密钥一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中，所述管理服务器装置具有与所述主密钥相同的主密钥；接收步骤，从所述管理服务器装置经由所述无线通信网络接收所述车载计算机的初始密钥与所述车载计算机的标识符的组；以及密钥存储步骤，存储通过所述接收步骤从所述管理服务器装置接收到的所述车载计算机的初始密钥与所述车载计算机的标识符的组。

[0033] (19)本发明的一个方式的计算机程序，所述计算机程序用于使在车辆具有的密钥生成装置的计算机执行：主密钥存储步骤，存储多个主密钥，该多个主密钥与和车载计算机的标识符一起用于生成初始密钥的多个主密钥相同，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及密钥生成步骤，使用通过所述主密钥存储步骤存储的多个主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成所述车载计算机的初始密钥。

[0034] (20)本发明的一个方式的计算机程序，其中，所述计算机程序用于使在车辆具有的第一值生成装置的计算机执行：第一主密钥存储步骤，存储与第一主密钥及第二主密钥中的所述第一主密钥相同的第一主密钥，所述第一主密钥及所述第二主密钥与车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车辆具有的所述车载计算机中；以及第一值生成步骤，使用通过所述第一主密钥存储步骤存储的第一主密钥和从所述车载计算机提供的所述车载计算机的标识符，来生成用于生成所述车载计算机的初始密钥的第一值，所述计算机程序用于使在所述车辆具有的初始密钥生成装置的计算机执行：第二主密钥存储步骤，存储与所述第一主密钥及所述第二主密钥中的所述第二主密钥相同的第二主密钥，所述第一主密钥及所述第二主密钥与所述车载计算机的标识符一起用于生成初始密钥，所述初始密钥被保存在所述车载计算机中；以及初始密钥生成步骤，使用通过所述第二主密钥存储步骤存储的第二主密钥和从所述第一值生成装置提供的所述第一值，来生成所述车载计算机的初始密钥。

[0035] 发明效果

[0036] 根据本发明，获得能够有助于对在机动车等车辆中保存的密钥进行管理、更新的效果。

附图说明

[0037] 图1是示出第一实施方式的机动车的框图。

[0038] 图2是示出第一实施方式的管理装置的框图。

[0039] 图3是示出第一实施方式的密钥存储部的框图。

[0040] 图4是示出第一实施方式的管理方法的图。

[0041] 图5是示出第一实施方式的管理方法的图。

[0042] 图6是示出第二实施方式的管理系统的框图。

[0043] 图7是示出第二实施方式的管理装置的框图。

[0044] 图8是示出第二实施方式的管理服务器装置的框图。

[0045] 图9是示出第二实施方式的管理方法的图。

[0046] 图10是示出第三实施方式的机动车的框图。

[0047] 图11是示出第四实施方式的管理系统的框图。

[0048] 图12是示出第五实施方式的管理方法的图。

[0049] 图13是示出第六实施方式的机动车的框图。

[0050] 图14是示出第六实施方式的管理方法的图。

[0051] 图15是示出第六实施方式的ECU初始密钥的共享方法(例1)的顺序图。

[0052] 图16是示出第六实施方式的ECU初始密钥的共享方法(例2)的顺序图。

[0053] 图17是示出第六实施方式的ECU初始密钥的共享方法(例3)的顺序图。

[0054] 图18是示出第六实施方式的机动车的变形例的框图。

具体实施方式

[0055] 以下,参照附图说明本发明的实施方式。需要说明的是,在以下示出的实施方式中,举出机动车作为车辆的例子来说明。

[0056] [第一实施方式]

[0057] 图1是示出第一实施方式的机动车1的框图。图1中,机动车1具有管理装置10和ECU50。管理装置10连接到控制用车载网络40。使用例如CAN(Controller Area Network;控制器区域网络)作为控制用车载网络40。已知CAN是车辆所搭载的通信网络的一种。本实施方式中,控制用车载网络40是CAN。控制用车载网络40上连接各种ECU50。ECU50是机动车1具有的车载计算机。ECU50例如是驱动类ECU、车体类ECU、安全控制类ECU等。管理装置10经由控制用车载网络40在与各ECU50之间交换数据。ECU50经由控制用车载网络40在与其他的ECU50之间交换数据。管理装置10具有安全元件20。

[0058] 图2是示出第一实施方式的管理装置10的框图。图2中,管理装置10具有控制部11、CAN接口12和安全元件20。这些各部能够交换数据。安全元件20具有密钥生成部21、密钥存储部22、验证部23和加密处理部24。

[0059] 控制部11具有管理装置10的控制功能。CAN接口12是与ECU50进行通信的通信部。CAN接口12与控制用车载网络40连接,经由控制用车载网络40与各ECU50交换数据。安全元件20具有防篡改性(Tamper Resistant)。

[0060] 在安全元件20中,密钥生成部21生成密钥。密钥存储部22存储密钥。验证部23使用密钥进行数据或数据交换对象等的验证。加密处理部24使用密钥进行数据的加密及加密数据的解密。

[0061] 图3是示出图2所示的密钥存储部22的结构例的框图。图3中,密钥存储部22具有主密钥存储部31和ECU初始密钥存储部32。

[0062] 主密钥存储部31存储主密钥MASTER_KEY。主密钥MASTER_KEY在管理装置10的制造工序等被安全地写入管理装置10的安全元件20中。ECU初始密钥存储部32将ECU初始密钥与ECU标识符关联地存储。

[0063] 下面,说明第一实施方式的ECU初始密钥的管理方法。

[0064] [向ECU写入ECU初始密钥的阶段]

[0065] 参照图4,说明向ECU50写入ECU初始密钥的阶段。图4是示出第一实施方式的管理方法的图。

[0066] 图4中,初始密钥写入装置301设置在ECU50的制造工厂内的房间300中。房间300是确保信息安全性的房间。初始密钥写入装置301具有主密钥MASTER_KEY。主密钥MASTER_KEY

被事先设定在初始密钥写入装置301中。对于初始密钥写入装置301的主密钥MASTER_KEY的设定被安全地执行。初始密钥写入装置301具有的主密钥MASTER_KEY和在机动车1的管理装置10的安全元件20的密钥存储部22中存储的主密钥MASTER_KEY是相同的。该主密钥MASTER_KEY被安全地管理。

[0067] 初始密钥写入装置301具有用于在与ECU50之间交换数据的ECU连接接口。初始密钥写入装置301在与连接到ECU连接接口的ECU50之间交换数据。需要说明的是，此处，初始密钥写入装置301具有三个ECU连接接口，通过该ECU连接接口可以同时与三个ECU50连接。

[0068] 作为机动车1搭载的ECU50，图4中示出三个ECU50。分别将这三个ECU50称为ECU_A_50、ECU_B_50、ECU_C_50。此处举出ECU_A_50、ECU_B_50及ECU_C_50的例子进行说明。

[0069] 初始密钥写入装置301通过ECU连接接口同时连接ECU_A_50、ECU_B_50及ECU_C_50。

[0070] (步骤S1)ECU_A_50、ECU_B_50及ECU_C_50分别向初始密钥写入装置301发送自己的ECU标识符。具体而言，ECU_A_50向初始密钥写入装置301发送ECU标识符ECU_ID_A。ECU_B_50向初始密钥写入装置301发送ECU标识符ECU_ID_B。ECU_C_50向初始密钥写入装置301发送ECU标识符ECU_ID_C。

[0071] 作为ECU标识符，例如，可以利用在制造时嵌入在作为构成ECU50的硬件的LSI等半导体集成电路中的标识符。例如，可以利用嵌入在ECU50的微型计算机的LSI中的标识符作为ECU标识符。

[0072] (步骤S2)初始密钥写入装置301使用主密钥MASTER_KEY和ECU标识符生成ECU初始密钥。具体而言，初始密钥写入装置301使用主密钥MASTER_KEY和ECU_A_50的ECU标识符ECU_ID_A，生成ECU_A_50的ECU初始密钥Key_A。初始密钥写入装置301使用主密钥MASTER_KEY和ECU_B_50的ECU标识符ECU_ID_B，生成ECU_B_50的ECU初始密钥Key_B。初始密钥写入装置301使用主密钥MASTER_KEY和ECU_C_50的ECU标识符ECU_ID_C，生成ECU_C_50的ECU初始密钥Key_C。

[0073] 说明ECU初始密钥的生成方法的例1、例2。

[0074] (ECU初始密钥的生成方法的例1)

[0075] 在ECU初始密钥的生成方法的例1中，利用散列(hash)函数。例如，可以将主密钥MASTER_KEY和ECU标识符的连结数据用于输入值来计算散列值，并将计算出的散列值用于ECU初始密钥。

[0076] (ECU初始密钥的生成方法的例2)

[0077] 在ECU初始密钥的生成方法的例2中，利用异或运算。例如，可以执行主密钥MASTER_KEY与ECU标识符的异或运算，并将运算结果的值“主密钥MASTER_KEY xor ECU标识符”用于ECU初始密钥。其中，“A xor B”是A与B的异或。

[0078] (步骤S3)初始密钥写入装置301将生成的ECU初始密钥写入对应的ECU50中。具体而言，初始密钥写入装置301将ECU初始密钥Key_A写入ECU_A_50中。初始密钥写入装置301将ECU初始密钥Key_B写入ECU_B_50中。初始密钥写入装置301将ECU初始密钥Key_C写入ECU_C_50中。

[0079] 在ECU初始密钥被写入后，ECU_A_50、ECU_B_50及ECU_C_50被搭载于机动车1中。

[0080] [管理装置的ECU初始密钥的共享阶段]

[0081] 参照图5，说明管理装置10的ECU初始密钥的共享阶段。图5是示出第一实施方式的管理方法的图。图5中，机动车1中搭载有通过上述的图4所示的初始密钥写入装置301被写入了ECU初始密钥的ECU_A_50、ECU_B_50及ECU_C_50。ECU_A_50具有ECU标识符ECU_ID_A及ECU初始密钥Key_A。ECU_B_50具有ECU标识符ECU_ID_B及ECU初始密钥Key_B。ECU_C_50具有ECU标识符ECU_ID_C及ECU初始密钥Key_C。机动车1中搭载的管理装置10的安全元件20的密钥存储部22存储有主密钥MASTER_KEY。该主密钥MASTER_KEY与初始密钥写入装置301具有的主密钥MASTER_KEY相同。

[0082] (步骤S101)ECU_A_50、ECU_B_50及ECU_C_50分别在被搭载于机动车1后初次通电时，经由控制用车载网络40向管理装置10发送自己的ECU标识符。具体而言，ECU_A_50向管理装置10发送ECU标识符ECU_ID_A。ECU_B_50向管理装置10发送ECU标识符ECU_ID_B。ECU_C_50向管理装置10发送ECU标识符ECU_ID_C。

[0083] 管理装置10经由控制用车载网络40，从ECU_A_50、ECU_B_50及ECU_C_50接收各ECU标识符ECU_ID_A、ECU_ID_B及ECU_ID_C。管理装置10中，接收到的ECU标识符ECU_ID_A、ECU_ID_B及ECU_ID_C被传给安全元件20。

[0084] (步骤S102)管理装置10的安全元件20中，密钥生成部21从密钥存储部22获取主密钥MASTER_KEY，并使用获取的主密钥MASTER_KEY和ECU标识符生成ECU初始密钥。具体而言，密钥生成部21使用主密钥MASTER_KEY和ECU_A_50的ECU标识符ECU_ID_A，生成ECU_A_50的ECU初始密钥Key_A。密钥生成部21使用主密钥MASTER_KEY和ECU_B_50的ECU标识符ECU_ID_B，生成ECU_B_50的ECU初始密钥Key_B。密钥生成部21使用主密钥MASTER_KEY和ECU_C_50的ECU标识符ECU_ID_C，生成ECU_C_50的ECU初始密钥Key_C。密钥生成部21的ECU初始密钥生成方法与上述的图4所示的初始密钥写入装置301的ECU初始密钥生成方法相同。

[0085] 管理装置10的安全元件20中，密钥存储部22将密钥生成部21生成的ECU初始密钥与ECU标识符关联地存储在ECU初始密钥存储部32中。具体而言，密钥存储部22将ECU_A_50的ECU初始密钥Key_A与ECU_A_50的ECU标识符ECU_ID_A关联地存储在ECU初始密钥存储部32中。密钥存储部22将ECU_B_50的ECU初始密钥Key_B与ECU_B_50的ECU标识符ECU_ID_B关联地存储在ECU初始密钥存储部32中。密钥存储部22将ECU_C_50的ECU初始密钥Key_C与ECU_C_50的ECU标识符ECU_ID_C关联地存储在ECU初始密钥存储部32中。由此，管理装置10的安全元件20与各ECU_A_50、ECU_B_50及ECU_C_50共享各ECU初始密钥Key_A、Key_B及Key_C。

[0086] 根据上述的第一实施方式，使用ECU50的ECU标识符和主密钥MASTER_KEY生成该ECU50的ECU初始密钥。由此，能够对各ECU50设定不同的ECU初始密钥。因此，即使某个ECU50的ECU初始密钥泄露，也可以防止对其他ECU50产生影响。

[0087] 另外，从机动车1中搭载的ECU50向该机动车1中搭载的管理装置10发送ECU标识符，管理装置10使用自身具有的主密钥MASTER_KEY和从ECU50接收到的ECU标识符生成该ECU50的ECU初始密钥。

[0088] 由此，管理装置10能够与各ECU50共享各ECU50所不同的ECU初始密钥。通过在管理装置10和ECU50共享的ECU初始密钥在该管理装置10与该ECU50之间，可以用于例如各种密钥交换中的加密及解密、数据交换中的加密及解密、通信对象的认证处理等。

[0089] 此外，可以存在多个主密钥MASTER_KEY。例如，当存在ECU50的多个制造商时，各制

造商持有不用的主密钥MASTER_KEY。下面说明该情况。图4所示的初始密钥写入装置301具有自己的制造商的主密钥MASTER_KEY。由此，通过初始密钥写入装置301被写入ECU50的ECU初始密钥是使用该ECU50的制造商的主密钥MASTER_KEY和该ECU50的ECU标识符而生成的。另外，机动车1中搭载的管理装置10的安全元件20的密钥存储部22存储有各制造商的主密钥MASTER_KEY。管理装置10的安全元件20中，密钥生成部21从密钥存储部22获取与从ECU50接收的ECU标识符对应的制造商的主密钥MASTER_KEY。ECU50的ECU标识符是能够识别该ECU50的制造商的结构。例如，ECU50的ECU标识符包括该ECU50的制造商的标识符。密钥生成部21使用与从ECU50接收的ECU标识符对应的制造商的主密钥MASTER_KEY和该ECU标识符来生成ECU初始密钥。由密钥生成部21生成的ECU初始密钥与该ECU标识符进行关联并被存储在ECU初始密钥存储部32中。

[0090] 另外，可以使机动车1中搭载的ECU50作为管理装置10发挥功能。作为管理装置10发挥功能的ECU50具有安全元件20。

[0091] [第二实施方式]

[0092] 图6是示出第二实施方式的管理系统的框图。对图6中与图1的各部对应的部分标记相同的符号，并省略其说明。图6中，管理系统具有管理装置10a和管理服务器装置80。管理装置10a设置在机动车1中。管理装置10a通过无线通信线路3连接到无线通信网络2。管理服务器装置80通过无线通信网络2的通信运营商的通信线路4连接到无线通信网络2。管理服务器装置80由例如无线通信网络2的通信运营商进行设置。管理装置10a与管理服务器装置80经由无线通信网络2进行通信。

[0093] 为了利用无线通信网络2，需要写有无线通信网络2的订户信息的SIM(Subscriber Identity Module;订户身份模块)或eSIM(Embedded Subscriber Identity Module;嵌入式订户身份模块)。管理装置10a具有SIM_20a。SIM_20a是写有无线通信网络2的订户信息的SIM。因此，管理装置10a能够通过使用SIM_20a而利用无线通信网络2。管理装置10a通过使用SIM_20a建立的无线通信线路3连接到无线通信网络2。SIM_20a是安全元件。

[0094] 此外，可以在管理装置10a与管理服务器装置80之间经由无线通信网络2建立专用线，管理装置10a与管理服务器装置80经由专用线来发送接收数据。

[0095] 机动车1中，管理装置10a连接到控制用车载网络40。本实施方式中，控制用车载网络40是CAN。控制用车载网络40上连接各种ECU50。管理装置10a经由控制用车载网络40在与各ECU50之间交换数据。

[0096] 图7是示出第二实施方式的管理装置10a的框图。对图7中与图2的各部对应的部分标记相同的符号，并省略其说明。图7中，管理装置10a具有控制部11、CAN接口12、无线通信部13和SIM_20a。这些各部可以交换数据。SIM_20a具有密钥生成部21、密钥存储部22、验证部23和加密处理部24。

[0097] SIM_20a是安全元件，具有防篡改性。需要说明的是，可以利用eSIM来代替SIM_20a作为安全元件。SIM及eSIM是计算机的一种，通过计算机程序实现期望的功能。

[0098] 无线通信部13通过无线通信发送接收数据。SIM_20a是写有无线通信网络2的订户信息的SIM。因此，无线通信部13通过使用SIM_20a，经由无线通信线路3连接到无线通信网络2。

[0099] 第二实施方式中，管理装置10a不具有主密钥MASTER_KEY。因此，在图7所示的管理

装置10a中SIM_20a的密钥存储部22只具有上述的图3所示的密钥存储部22的结构中的ECU初始密钥存储部32。因此，在图7所示的管理装置10a中，SIM_20a的密钥存储部22不具有主密钥存储部31。ECU初始密钥存储部32将ECU初始密钥与ECU标识符关联地存储。

[0100] 图8是示出第二实施方式的管理服务器装置80的框图。图8中，管理服务器装置80具有通信部81、存储部82、管理部83和密钥生成部84。

[0101] 这些各部可以交换数据。通信部81经由通信线路4发送接收数据。通信部81经由通信线路4连接到无线通信网络2。通信部81经由无线通信网络2与管理装置10a进行通信。存储部82存储主密钥MASTER_KEY等数据。管理部83进行有关机动车1的管理。密钥生成部84生成密钥。

[0102] 下面，说明第二实施方式的ECU初始密钥的管理方法。

[0103] [向ECU写入ECU初始密钥的阶段]

[0104] 向ECU写入ECU初始密钥的阶段与上述的参照图4说明的第一实施方式相同。但是，第二实施方式中，管理服务器装置80的存储部82存储有与初始密钥写入装置301中保存的主密钥相同的主密钥MASTER_KEY。机动车1中搭载的管理装置10a不具有主密钥MASTER_KEY。

[0105] [管理装置的ECU初始密钥的共享阶段]

[0106] 参照图9，说明管理装置10a的ECU初始密钥的共享阶段。图9是示出第二实施方式的管理方法的图。图9中，机动车1中搭载有通过上述的图4所示的初始密钥写入装置301写入有ECU初始密钥的ECU_A_50、ECU_B_50及ECU_C_50。

[0107] ECU_A_50具有ECU标识符ECU_ID_A及ECU初始密钥Key_A。ECU_B_50具有ECU标识符ECU_ID_B及ECU初始密钥Key_B。ECU_C_50具有ECU标识符ECU_ID_C及ECU初始密钥Key_C。机动车1中搭载有管理装置10a。管理服务器装置80存储有主密钥MASTER_KEY。该主密钥MASTER_KEY与初始密钥写入装置301具有的主密钥MASTER_KEY相同。

[0108] (步骤S201)ECU_A_50、ECU_B_50及ECU_C_50分别在被搭载于机动车1后初次通电时，经由管理装置10a向管理服务器装置80发送自己的ECU标识符。具体而言，ECU_A_50经由控制用车载网络40向管理装置10a发送ECU标识符ECU_ID_A。管理装置10a经由无线通信网络2，向管理服务器装置80发送从ECU_A_50经由控制用车载网络40接收到的ECU标识符ECU_ID_A。ECU_B_50也是同样，经由管理装置10a向管理服务器装置80发送ECU标识符ECU_ID_B。ECU_C_50也是同样，经由管理装置10a向管理服务器装置80发送ECU标识符ECU_ID_C。

[0109] 管理服务器装置80从机动车1的管理装置10a经由无线通信网络2接收ECU_A_50、ECU_B_50及ECU_C_50的各ECU标识符ECU_ID_A、ECU_ID_B及ECU_ID_C。

[0110] (步骤S202)管理服务器装置80的密钥生成部84使用从机动车1的管理装置10a接收到的ECU标识符和在存储部82中存储的主密钥MASTER_KEY生成ECU初始密钥。具体而言，密钥生成部84使用主密钥MASTER_KEY和ECU_A_50的ECU标识符ECU_ID_A，生成ECU_A_50的ECU初始密钥Key_A。密钥生成部84使用主密钥MASTER_KEY和ECU_B_50的ECU标识符ECU_ID_B，生成ECU_B_50的ECU初始密钥Key_B。密钥生成部84使用主密钥MASTER_KEY和ECU_C_50的ECU标识符ECU_ID_C，生成ECU_C_50的ECU初始密钥Key_C。密钥生成部84的ECU初始密钥生成方法与上述的图4所示的初始密钥写入装置301的ECU初始密钥生成方法相同。

[0111] (步骤S203)管理服务器装置80将使用主密钥MASTER_KEY和ECU标识符生成的ECU

初始密钥与该ECU标识符一起，经由无线通信网络2向机动车1的管理装置10a发送。具体而言，管理服务器装置80将ECU标识符ECU_ID_A与ECU初始密钥Key_A的组经由无线通信网络2向机动车1的管理装置10a发送。管理服务器装置80将ECU标识符ECU_ID_B与ECU初始密钥Key_B的组经由无线通信网络2向机动车1的管理装置10a发送。管理服务器装置80将ECU标识符ECU_ID_C与ECU初始密钥Key_C的组经由无线通信网络2向机动车1的管理装置10a发送。

[0112] 机动车1的管理装置10a从管理服务器装置80经由无线通信网络2接收ECU标识符ECU_ID_A与ECU初始密钥Key_A的组、ECU标识符ECU_ID_B与ECU初始密钥Key_B的组以及ECU标识符ECU_ID_C与ECU初始密钥Key_C的组。

[0113] (步骤S204)管理装置10a的SIM_20a中，密钥存储部22将从管理服务器装置80接收到的ECU标识符与ECU初始密钥的组存储在ECU初始密钥存储部32中。具体而言，密钥存储部22将与从管理服务器装置80接收到的ECU_A_50的ECU标识符ECU_ID_A关联地以该ECU标识符ECU_ID_A的组的形式从管理服务器装置80接收到的ECU初始密钥Key_A存储在ECU初始密钥存储部32中。将与从管理服务器装置80接收到的ECU_B_50的ECU标识符ECU_ID_B关联地以该ECU标识符ECU_ID_B的组的形式从管理服务器装置80接收到的ECU初始密钥Key_B存储在ECU初始密钥存储部32中。将与从管理服务器装置80接收到的ECU_C_50的ECU标识符ECU_ID_A关联地以该ECU标识符ECU_ID_C的组的形式从管理服务器装置80接收到的ECU初始密钥Key_C存储在ECU初始密钥存储部32中。由此，管理装置10a的SIM_20a与各ECU_A_50、ECU_B_50及ECU_C_50共享各ECU初始密钥Key_A、Key_B及Key_C。

[0114] 根据上述的第二实施方式，使用ECU50的ECU标识符和主密钥MASTER_KEY生成该ECU50的ECU初始密钥。由此，可以对各ECU50设定不同的ECU初始密钥。因此，即使某一ECU50的ECU初始密钥泄露，也能防止对其他的ECU50产生影响。

[0115] 另外，从机动车1中搭载的管理装置10a向管理服务器装置80发送在机动车1中搭载的ECU50的ECU标识符，管理服务器装置80使用自己具有的主密钥MASTER_KEY和从管理装置10a接收到的ECU标识符生成ECU初始密钥，并向管理装置10a发送生成的ECU初始密钥。由此，管理装置10a能够与各ECU50共享各ECU50所不同的ECU初始密钥。通过管理装置10a与ECU50共享的ECU初始密钥在该管理装置10a与该ECU50之间，例如可以用于各种密钥交换中的加密及解密、数据交换中的加密及解密、通信对象的认证处理等。

[0116] 此外，可以存在多个主密钥MASTER_KEY。例如，当存在ECU50的多个制造商时，各制造商持有不同的主密钥MASTER_KEY。下面说明该情况。图4所示的初始密钥写入装置301具有自己的制造商的主密钥MASTER_KEY。由此，通过初始密钥写入装置301被写入ECU50的ECU初始密钥是使用该ECU50的制造商的主密钥MASTER_KEY和该ECU50的ECU标识符而生成的。另外，管理服务器装置80存储有各制造商的主密钥MASTER_KEY。管理服务器装置80使用与从机动车1的管理装置10a接收到的ECU标识符对应的制造商的主密钥MASTER_KEY和其ECU标识符生成ECU初始密钥。ECU50的ECU标识符是能够识别该ECU50的制造商的结构。例如，ECU50的ECU标识符包括该ECU50的制造商的标识符。由管理服务器装置80生成的ECU初始密钥与其ECU标识符关联地发送给管理装置10a。管理装置10a的SIM_20a中，密钥存储部22将从管理服务器装置80接收到的ECU标识符与ECU初始密钥的组存储在ECU初始密钥存储部32中。

[0117] 另外，可以使机动车1中搭载的ECU50作为管理装置10a发挥功能。作为管理装置10a发挥功能的ECU50具有无线通信部13和SIM_20a。

[0118] 上述的第二实施方式中，在管理装置的ECU初始密钥的共享阶段中，机动车1与管理服务器装置80通过无线进行通信。另一方面，上述的第一实施方式中，管理装置的ECU初始密钥的共享阶段在机动车1的内部封闭进行。因此，根据上述的第一实施方式，也可适用于无法进行无线通信的环境。

[0119] [第三实施方式]

[0120] 图10是示出第三实施方式的机动车1的框图。图10中，对与图1的各部对应的部分标记相同的符号，并省略其说明。相对于图1所示的机动车1，图10所示的机动车1还具有网关100、信息娱乐(Infotainment)设备110和通信装置120。通信装置120具有SIM_121。SIM_121是写有无线通信网络2的订户信息的SIM。因此，通信装置120能够通过使用SIM_121来利用无线通信网络2。通信装置120通过使用SIM_121建立的无线通信线路161连接到无线通信网络2。无线通信网络2经由通信线路162与互联网150连接。服务器装置140经由通信线路163连接到互联网150。通信装置120经由无线通信网络2与连接到互联网150的服务器装置140进行通信。

[0121] 机动车1的信息娱乐设备110经由通信装置120与服务器装置140发送接收数据。信息娱乐设备110与外部设备130连接，与外部设备130交换数据。作为外部设备130，例如，举出便携通信终端、视听设备等。

[0122] 机动车1中，网关100连接到控制用车载网络40。信息娱乐设备110经由网关100，与连接到控制用车载网络40的ECU50、管理装置10发送接收数据。网关100监控信息娱乐设备110与ECU50之间的数据的发送接收以及信息娱乐设备110与管理装置10之间的数据的发送接收。

[0123] 此外，可以使机动车1中搭载的ECU50作为管理装置10发挥功能。作为管理装置10发挥功能的ECU50具有安全元件20。

[0124] [第四实施方式]

[0125] 第四实施方式是上述的第二实施方式和第三实施方式的组合例。图11是示出第四实施方式的管理系统的框图。图11中，对与图6及图10的各部对应的部分标记相同的符号，并省略其说明。

[0126] 图11中，通信装置120通过无线通信线路161连接到无线通信网络2。通信装置120经由无线通信网络2与管理服务器装置80进行通信。管理装置10a经由网关100与通信装置120发送接收数据。管理装置10a经由通信装置120与管理服务器装置80发送接收数据。网关100监控通信装置120与管理装置10a之间的数据的发送接收。

[0127] 第四实施方式中，管理装置10a经由通信装置120与管理服务器装置80进行通信。因此，图11所示的管理装置10a可以不具有上述的图7所示的无线通信部13。在图11所示的管理装置10a中，当不具有无线通信部13时，安全元件20a可以不是SIM。图11所示的安全元件20a具有上述的图7所示的SIM_20a的各部21～24。

[0128] 此外，可以使机动车1中搭载的ECU50作为管理装置10a发挥功能。作为管理装置10a发挥功能的ECU50具有安全元件20a。

[0129] 上述的第四实施方式中，在管理装置的ECU初始密钥的共享阶段中，机动车1与管

理服务器装置80通过无线进行通信。另一方面，上述的第三实施方式中，管理装置的ECU初始密钥的共享阶段在机动车1的内部封闭进行。因此，根据上述的第三实施方式，也可适用于无法进行无线通信的环境。

[0130] [第五实施方式]

[0131] 图12是示出第五实施方式的管理方法的图。主密钥MASTER_KEY在多个装置间被共享。例如，上述的第一实施方式中，主密钥MASTER_KEY在初始密钥写入装置301与机动车1的管理装置10之间被共享。

[0132] 另外，上述的第二实施方式中，主密钥MASTER_KEY在初始密钥写入装置301与管理服务器装置80之间被共享。第五实施方式中，谋求在多个装置间安全地共享主密钥MASTER_KEY。

[0133] 主密钥MASTER_KEY由多个元素生成。图12的例中，主密钥MASTER_KEY是三个元素Key_x、Key_y及Key_z的异或“Key_x xor Key_y xor Key_z”。

[0134] 图12中例示出对初始密钥写入装置301写入主密钥MASTER_KEY的情况。下面，参照图12说明第五实施方式的管理方法。

[0135] (步骤S301)将主密钥MASTER_KEY的三个元素Key_x、Key_y及Key_z从发送源分别通过不同的发送路径发送给发送目的地的初始密钥写入装置301的管理员。例如，元素Key_x通过邮件发送，元素Key_y是利用与邮件不同的发送公司发送，而元素Key_z是发送源的负责人自己携带到发送目的地。

[0136] (步骤S302)初始密钥写入装置301的管理员分别对初始密钥写入装置301输入通过不同的发送路径接收到的三个元素Key_x、Key_y及Key_z。

[0137] (步骤S303)初始密钥写入装置301使用分别输入的三个元素Key_x、Key_y及Key_z执行异或运算。初始密钥写入装置301将该运算结果的异或“Key_x xor Key_y xor Key_z”用于主密钥MASTER_KEY。

[0138] 对于主密钥MASTER_KEY的共享目的地的各装置，按照上述的图12的顺序共享主密钥MASTER_KEY。由此，能够在多个装置间安全地共享主密钥MASTER_KEY。

[0139] 需要说明的是，当主密钥MASTER_KEY泄露时，通过改写各装置中保存的主密钥MASTER_KEY来保证安全性。在上述的第一实施方式的情况下，在图1所示的机动车1搭载的管理装置10的安全元件20中保存的主密钥MASTER_KEY的改写通过例如管理装置10的交换来进行。在上述的第三实施方式的情况下，在图10所示的机动车1搭载的管理装置10的安全元件20中保存的主密钥MASTER_KEY的改写例如通过通信装置120经由无线通信网络2进行。在上述的第二实施方式及第四实施方式的情况下，在图6及图11所示的管理服务器装置80中保存的主密钥MASTER_KEY的改写按照上述的图12的顺序进行。

[0140] 另外，当主密钥MASTER_KEY泄露时，优选，除改写在各装置中保存的主密钥MASTER_KEY以外，还更新ECU初始密钥。下面说明该ECU初始密钥的更新方法。

[0141] 在上述的第一实施方式及第三实施方式的情况下，图1及图10所示的机动车1中搭载的管理装置10的安全元件20的密钥生成部21使用新主密钥MASTER_KEY和ECU50的ECU标识符生成该ECU50的新ECU初始密钥。新ECU初始密钥通过密钥交换密钥进行加密后，从管理装置10向ECU50安全地发送。密钥交换密钥是管理装置10为了对认证过的ECU50交换密钥而提供的密钥。ECU50通过密钥交换密钥对从管理装置10接收到的加密后的新ECU初始密钥进

行解密，并将自己保存的ECU初始密钥更新为解密结果的新ECU初始密钥。

[0142] 此外，对于未认证的ECU50进行回收，并通过初始密钥写入装置301进行ECU初始密钥的更新。作为未认证的ECU50，例如，举出未在机动车1中搭载的ECU50。初始密钥写入装置301使用新主密钥MASTER_KEY和回收的ECU50的ECU标识符生成该ECU50的新ECU初始密钥。初始密钥写入装置301将生成的新ECU初始密钥写入该ECU50，并将该ECU50中保存的ECU初始密钥更新为新ECU初始密钥。

[0143] 在上述的第二实施方式及第四实施方式的情况下，图6及图11所示的管理服务器装置80使用新主密钥MASTER_KEY和ECU50的ECU标识符生成该ECU50的新ECU初始密钥。ECU50的新ECU初始密钥与该ECU50的ECU标识符一起，经由无线通信网络2从管理服务器装置80被发送给管理装置10a。管理装置10a保存从管理服务器装置80接收到的ECU标识符与新ECU初始密钥的组。另外，管理装置10a将与从管理服务器装置80接收到的ECU标识符一起从管理服务器装置80接收到的新ECU初始密钥通过密钥交换密钥进行加密并发送给该ECU标识符的ECU50。密钥交换密钥是管理装置10a为了对认证过的ECU50交换密钥而提供的密钥。ECU50通过密钥交换密钥将从管理装置10a接收到的加密后的新ECU初始密钥进行解密，并将自己保存的ECU初始密钥更新为解密结果的新ECU初始密钥。需要说明的是，如上所述，对于未认证的ECU50进行回收，并通过初始密钥写入装置301进行ECU初始密钥的更新。

[0144] 以上，参照附图详细说明了本发明的实施方式，但具体结构并不限于该实施方式，也可以包括不脱离本发明的主旨的范围内的设计变更等。

[0145] 例如，上述的实施方式中，作为安全元件，举出了使用SIM或eSIM的例，但不限于此。作为安全元件，例如，也可以使用具有防篡改性的加密处理芯片。作为具有防篡改性的加密处理芯片，例如，已知被称为HSM(Hardware Security Module;硬件安全模块)、TPM(Trusted Platform Module;可信平台模块)或SHE(Secure Hardware Extension;安全硬件扩展)等的加密处理芯片。关于TPM，例如在非专利文献3中有所记载。例如，可以将HSM、TPM或SHE用作管理装置10的安全元件20。或者，可以将SIM或eSIM用作管理装置10的安全元件20。或者，可以将HSM、TPM或SHE用作上述的第四实施方式的图11所示的管理装置10a的安全元件20a。

[0146] 下面说明本发明的其他实施方式。

[0147] [第六实施方式]

[0148] 图13是示出第六实施方式的机动车1001的框图。图13中，机动车1001具有第一ECU1010和多个第二ECU1020。第一ECU1010及第二ECU1020是机动车1001具有的车载计算机。第一ECU1010是机动车1001搭载的ECU中具有网关功能的ECU。第二ECU1020是机动车1001搭载的ECU中具有发动机控制等功能的ECU。作为第二ECU1020，例如，存在具有发动机控制功能的ECU、具有手柄控制功能的ECU、具有制动器控制功能的ECU等。

[0149] 第一ECU1010和多个第二ECU1020连接到机动车1001具有的CAN(Controller Area Network;控制器区域网络)1030。CAN1030是通信网络。已知CAN是车辆搭载的通信网络的一种。

[0150] 第一ECU1010经由CAN1030在与各第二ECU1020之间交换数据。第二ECU1020经由CAN1030在与其他的第二ECU1020之间交换数据。

[0151] 此外，作为车辆中搭载的通信网络，机动车1001可以具有CAN以外的通信网络，并

经由CAN以外的通信网络进行第一ECU1010与第二ECU1020之间的数据交换以及第二ECU1020之间的数据交换。例如，机动车1001中可以具有LIN(Local Interconnect Network;本地互连网络)。另外，机动车1001中可以具有CAN和LIN。另外，机动车1001中还可以具有连接到LIN的第二ECU1020。

[0152] 另外，第一ECU1010可以连接到CAN和LIN。另外，第一ECU1010可以经由CAN在与连接到该CAN的第二ECU1020之间交换数据，并且，第一ECU1010可以经由LIN在与连接到该LIN的第二ECU1020之间交换数据。另外，第二ECU1020间可以经由LIN交换数据。

[0153] 机动车1001具有诊断端口1060。作为诊断端口1060，例如可以使用OBD端口。诊断端口1060上可以连接诊断终端1065。诊断端口1060连接到第一ECU1010。第一ECU1010与连接到诊断端口1060的诊断终端1065经由诊断端口1060交换数据。

[0154] 机动车1001具有信息娱乐(Infotainment)设备1040。作为信息娱乐设备1040，例如，举出具有导航功能、位置信息服务功能、音乐或动画等多媒体播放功能、语音通信功能、数据通信功能、互联网连接功能等的设备。信息娱乐设备1040连接到第一ECU1010。第一ECU1010将从信息娱乐设备1040输入的信息发送给第二ECU1020。

[0155] 机动车1001具有TCU(Tele Communication Unit;通信单元)1050。TCU1050是通信装置。TCU1050具有通信模块1051。通信模块1051利用无线通信网络进行无线通信。通信模块1051具有SIM(Subscriber Identity Module;订户身份模块)1052。SIM1052是写有用于利用无线通信网络的信息的SIM。通信模块1051通过使用SIM1052能够连接到该无线通信网络并进行无线通信。

[0156] SIM1052具有存储密钥的密钥存储部1053。此外，作为SIM1052，可以使用eSIM(Embedded Subscriber Identity Module;嵌入式订户身份模块)。SIM及eSIM具有防篡改性(Tamper Resistant)。SIM及eSIM是安全元件的例。安全元件具有防篡改性。SIM及eSIM是计算机的一种，通过计算机程序实现期望的功能。

[0157] TCU1050连接到第一ECU1010。第一ECU1010与TCU1050的通信模块1051交换数据。

[0158] 需要说明的是，图13的结构中通过将第一ECU1010与TCU1050直接连接而在第一ECU1010与通信模块1051之间交换数据，但不限于此。例如，可以将TCU1050连接到信息娱乐设备1040，第一ECU1010经由信息娱乐设备1040与TCU1050的通信模块1051交换数据。或者，可以将TCU1050代替诊断终端1065来连接到诊断端口1060，第一ECU1010经由诊断端口1060与连接到该诊断端口1060的TCU1050的通信模块1051交换数据。或者，第一ECU1010可以具有包括SIM1052的通信模块1051。在第一ECU1010具有包括SIM1052的通信模块1051的情况下，机动车1001可以不具有TCU1050。

[0159] 第一ECU1010具有主运算器1011和HSM(Hardware Security Module;硬件安全模块)1012。主运算器1011执行用于实现第一ECU1010的功能的计算机程序。HSM1012具有加密处理功能。HSM1012具有防篡改性。HSM1012具有用于存储密钥的密钥存储部1013。主运算器1011使用HSM1012。

[0160] 第二ECU1020具有主运算器1021和SHE(Secure Hardware Extension;安全硬件扩展)1022。主运算器1021执行用于实现第二ECU1020的功能的计算机程序。SHE1022具有加密处理功能。SHE1022具有防篡改性。SHE1022具有用于存储密钥的密钥存储部1023。主运算器1021使用SHE1022。

[0161] 机动车1001具有的车载计算机系统1002的第一ECU1010和多个第二ECU1020连接到CAN1030。第一ECU1010具有网关功能，监控车载计算机系统1002的内部与外部之间的通信。此外，车载计算机系统1002还可以包括通信模块1051的SIM1052。

[0162] 接着，说明本实施方式的管理方法。

[0163] [向ECU写入ECU初始密钥的阶段]

[0164] 参照图14，说明本实施方式的向ECU写入ECU初始密钥的阶段。图14是示出第六实施方式的管理方法的图。第六实施方式中，使用多个主密钥来生成ECU初始密钥。

[0165] 图14中，写入装置301-1设置在第一制造工厂内的房间300-1中。写入装置301-2设置在第二制造工厂内的房间300-2中。房间300-1及房间300-2是确保了信息安全性的房间。第一制造工厂例如是制造ECU本身的ECU制造商的工厂。第二制造工厂例如是将由ECU制造商供给的ECU作为自己的品牌ECU用于机动车的OEM(Original Equipment Manufacturing)供应商的工厂。

[0166] 写入装置301-1具有第一主密钥MASTER_KEY1。第一主密钥MASTER_KEY1事先设定在写入装置301-1中。对于写入装置301-1的第一主密钥MASTER_KEY1的设定被安全地执行。写入装置301-2具有第二主密钥MASTER_KEY2。第二主密钥MASTER_KEY2事先设定在写入装置301-2中。对于写入装置301-2的第二主密钥MASTER_KEY2的设定被安全地执行。

[0167] 写入装置301-1及301-2具有用于在与ECU之间交换数据的ECU连接接口。写入装置301-1及301-2在与连接到ECU连接接口的ECU之间交换数据。

[0168] 图14中，示出一个ECU作为机动车1001中搭载的ECU。将这一个ECU称为ECU_D。ECU_D可以是第一ECU1010，或者，也可以是第二ECU1020。

[0169] (步骤S501)在第一制造工厂内的房间300-1中，ECU_D连接到写入装置301-1。ECU_D向写入装置301-1发送自己的ECU标识符ECU_ID_D。

[0170] 作为ECU标识符，例如，可以利用在制造作为构成ECU的硬件的LSI等半导体集成电路时嵌入的标识符。例如，可以将在ECU的微型计算机的LSI中嵌入的标识符用于ECU标识符。

[0171] (步骤S502)写入装置301-1使用ECU标识符和第一主密钥MASTER_KEY1生成第一值。具体而言，写入装置301-1使用ECU_D的ECU标识符ECU_ID_D和第一主密钥MASTER_KEY1，生成ECU_D的第一值。可以计算ECU标识符和第一主密钥MASTER_KEY1的摘要(digest)作为第一值。作为摘要的计算方法，例如，可以利用散列(hash)函数，或者，也可以利用异或运算。此处利用散列函数作为第一值的计算方法。具体而言，写入装置301-1将ECU_D的ECU标识符ECU_ID_D和第一主密钥MASTER_KEY1用于散列函数的输入值来计算散列值，并将计算出的散列值hash(ECU_ID_D,MASTER_KEY1)作为ECU_D的第一值。

[0172] (步骤S503)写入装置301-1将生成的第一值写入ECU。具体而言，写入装置301-1将第一值hash(ECU_ID_D,MASTER_KEY1)写入ECU_D。ECU_D在写入了第一值hash(ECU_ID_D,MASTER_KEY1)后被运往第二制造工厂。

[0173] (步骤S504)在第二制造工厂内的房间300-2中，ECU_D连接到写入装置301-2。ECU_D向写入装置301-2发送自己的第一值hash(ECU_ID_D,MASTER_KEY1)。

[0174] (步骤S505)写入装置301-2使用第一值和第二主密钥MASTER_KEY2生成ECU初始密钥。具体而言，写入装置301-2使用ECU_D的第一值hash(ECU_ID_D,MASTER_KEY1)和第二主

密钥MASTER_KEY2，生成ECU_D的ECU初始密钥。可以计算第一值和第二主密钥MASTER_KEY2的摘要作为ECU初始密钥。作为摘要的计算方法，例如，可以利用散列函数，或者，也可以利用异或运算。此处，利用散列函数作为ECU初始密钥的计算方法。具体而言，写入装置301-2将ECU_D的第一值hash(ECU_ID_D,MASTER_KEY1)和第二主密钥MASTER_KEY2用于散列函数的输入值来计算散列值，并将计算出的散列值hash(hash(ECU_ID_D,MASTER_KEY1),MASTER_KEY2)作为ECU_D的ECU初始密钥Key_D。

[0175] (步骤S506)写入装置301-2将生成的ECU初始密钥写入ECU。具体而言，写入装置301-2将ECU初始密钥Key_D写入ECU_D。ECU_D在写入了ECU初始密钥Key_D后被搭载于机动车1001中。

[0176] 根据本实施方式，使用ECU的ECU标识符和多个主密钥生成该ECU的ECU初始密钥。由此，提高ECU初始密钥的安全性。下面说明这一效果。

[0177] 例如，考虑制造ECU本身的ECU制造商保管第一主密钥MASTER_KEY1，而将由ECU制造商供给的ECU作为自己的品牌ECU并用于机动车的OEM供应商保管第二主密钥MASTER_KEY2的情况。该情况下，ECU制造商和OEM供应商分别各自根据ECU的ECU标识符和自己的一个主密钥生成该ECU的ECU初始密钥并写入ECU。结果，因一个主密钥泄露而导致在使用这个主密钥的制造商中被写入ECU的ECU初始密钥可能发生泄露。结果，当ECU制造商的第一主密钥MASTER_KEY1泄露时，有可能产生对使用在ECU制造商中被写入了ECU初始密钥的ECU的所有OEM供应商更换ECU等的负担。另外，当OEM供应商的第二主密钥MASTER_KEY2泄露时，有可能产生对搭载有在OEM供应商中被写入了ECU初始密钥的ECU的所有车型更换ECU等的负担。

[0178] 对此，根据本实施方式，由于使用多个主密钥来生成ECU初始密钥，因此只要不是所有的主密钥都泄露，就能防止ECU初始密钥的泄露。在ECU制造商保管第一主密钥MASTER_KEY1，而OEM供应商保管第二主密钥MASTER_KEY2的情况下，当使用这两个主密钥MASTER_KEY1及MASTER_KEY2来生成ECU初始密钥时，即使这两个主密钥MASTER_KEY1及MASTER_KEY2中的一个主密钥泄露，也能防止ECU初始密钥的泄露。另外，当发现这两个主密钥MASTER_KEY1及MASTER_KEY2中的任一主密钥发生泄露时，通过在另一个主密钥泄露前更新泄露的主密钥，可以将ECU初始密钥的泄露防范于未然。另外，当这两个主密钥MASTER_KEY1及MASTER_KEY2都泄露时，可以控制使ECU初始密钥的泄露仅对该ECU制造商与该OEM供应商的组合建立的ECU产生影响。结果，能够减轻ECU制造商、OEM供应商等的更换ECU等的负担。

[0179] [ECU初始密钥的共享阶段]

[0180] 接着，举出ECU初始密钥的共享方法的例子来说明本实施方式的ECU初始密钥的共享阶段。

[0181] [ECU初始密钥的共享方法的例1]

[0182] 参照图15说明ECU初始密钥的共享方法的例1。图15是示出第六实施方式的ECU初始密钥的共享方法(例1)的顺序图。图15中，机动车1001中搭载有通过上述的图14所示的写入装置301-2写有ECU初始密钥Key_H的第一ECU1010，和通过该写入装置301-2写有ECU初始密钥Key_S的第二ECU1020。第一ECU1010具有ECU标识符ECU_ID_H。第一ECU1010中，HSM1012的密钥存储部1013存储有ECU初始密钥Key_H。第二ECU1020具有ECU标识符ECU_ID_S。第二ECU1020中，SHE1022的密钥存储部1023存储有ECU初始密钥Key_S。

[0183] 机动车1001中，TCU1050内的通信模块1051具有的SIM1052的密钥存储部1053存储

有第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2。在制造SIM1052时等，第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2被安全地存储在该SIM1052中。SIM1052的密钥存储部1053中存储的第一主密钥MASTER_KEY1与上述的图14所示的写入装置301-1具有的第一主密钥MASTER_KEY1相同。SIM1052的密钥存储部1053中存储的第二主密钥MASTER_KEY2与上述的图14所示的写入装置301-2具有的第二主密钥MASTER_KEY2相同。即，SIM1052的密钥存储部1053存储有与为了生成第一ECU1010的ECU初始密钥Key_H及第二ECU1020的ECU初始密钥Key_S而使用的第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2相同的第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2。

[0184] 以下的说明中，第一ECU1010与TCU1050内的通信模块1051的SIM1052交换数据。

[0185] (步骤S601)第一ECU1010向SIM1052提供自己的ECU标识符ECU_ID_H。该提供的时刻例如是第一ECU1010被搭载于机动车1001后初次通电时等。

[0186] (步骤S602)SIM1052使用从第一ECU1010提供的ECU标识符ECU_ID_H和密钥存储部1053中存储的第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2，生成第一ECU1010的ECU初始密钥Key_H。该SIM1052的ECU初始密钥生成方法与上述的图14所示的写入装置301-1及301-2的ECU初始密钥生成方法相同。密钥存储部1053将生成的第一ECU1010的ECU初始密钥Key_H与该第一ECU1010的ECU标识符ECU_ID_H关联地存储。由此，在SIM1052与第一ECU1010之间共享相同的ECU初始密钥Key_H。该被共享的ECU初始密钥Key_H例如被用于在SIM1052与第一ECU1010的HSM1012之间交换的数据的加密等。

[0187] (步骤S603)第二ECU1020经由第一ECU1010，向SIM1052提供自己的ECU标识符ECU_ID_S。该提供的时刻例如是第二ECU1020被搭载于机动车1001后初次通电时等。

[0188] (步骤S604)SIM1052使用从第二ECU1020提供的ECU标识符ECU_ID_S和密钥存储部1053中存储的第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2，生成第二ECU1020的ECU初始密钥Key_S。该SIM1052的ECU初始密钥生成方法与上述的图14所示的写入装置301-1及301-2的ECU初始密钥生成方法相同。

[0189] (步骤S605)SIM1052通过在密钥存储部1053中存储的第一ECU1010的ECU初始密钥Key_H来对生成的ECU初始密钥Key_S进行加密，生成加密数据Key_H(Key_S)。SIM1052向第一ECU1010发送该加密数据Key_H(Key_S)。此时，SIM1052可以向第一ECU1010发送加密数据Key_H(Key_S)与第二ECU1020的ECU标识符ECU_ID_S的组。

[0190] 第一ECU1010向HSM1012提供从SIM1052接收到的加密数据Key_H(Key_S)。HSM1012通过密钥存储部1013中存储的ECU初始密钥Key_H来解密该加密数据Key_H(Key_S)。

[0191] 作为该解密结果，得到第二ECU1020的ECU初始密钥Key_S。HSM1012的密钥存储部1013将该第二ECU1020的ECU初始密钥Key_S与第二ECU1020的ECU标识符ECU_ID_S关联地存储。由此，在第一ECU1010与第二ECU1020之间共享相同的ECU初始密钥Key_S。该共享的ECU初始密钥Key_S例如用于在第一ECU1010的HSM1012与第二ECU1020的SHE1022之间交换的数据的加密等。

[0192] 第一ECU1010中，与第二ECU1020的ECU初始密钥Key_S进行关联的第二ECU1020的ECU标识符ECU_ID_S可以在步骤S603中传输第二ECU1020的ECU标识符ECU_ID_S时记录该ECU标识符ECU_ID_S，或者，也可以使用在从SIM1052接收到的加密数据Key_H(Key_S)与第二ECU1020的ECU标识符ECU_ID_S的组中包括的ECU标识符ECU_ID_S。

[0193] 上述的ECU初始密钥的共享方法的例1中，SIM1052是密钥生成装置的例。另外，SIM1052和HSM1012是密钥管理系统的例。

[0194] 需要说明的是，上述的ECU初始密钥的共享方法的例1中，SIM1052具有第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2，该SIM1052使用该第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2生成ECU初始密钥，但不限于此。也可以是第一ECU1010的HSM1012的密钥存储部1013存储第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2，该HSM1012使用该第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2生成ECU初始密钥。该情况下，HSM1012是密钥生成装置的例。另外，HSM1012是密钥管理系统的例。

[0195] [ECU初始密钥的共享方法的例2]

[0196] 参照图16说明ECU初始密钥的共享方法的例2。图16是示出第六实施方式的ECU初始密钥的共享方法(例2)的顺序图。

[0197] 上述的ECU初始密钥的共享方法的例1中，将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2保管在同一SIM1052(安全元件)中。本ECU初始密钥的共享方法的例2中，将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同标准(Specification)的安全元件中。具体而言，图16中，第一ECU1010的HSM1012将第一主密钥MASTER_KEY1存储在密钥存储部1013中，通信模块1051的SIM1052将第二主密钥MASTER_KEY2存储在密钥存储部1053中。在制造HSM1012时等，第一主密钥MASTER_KEY1被安全地存储在该HSM1012中。在制造SIM1052时等，第二主密钥MASTER_KEY2被安全地存储在SIM1052中。

[0198] 除该主密钥的分散管理相关的点以外，通信模块1051的SIM1052、第一ECU1010的HSM1012以及第二ECU1020的SHE1022与图15所示的ECU初始密钥的共享方法的例1的结构相同。下面，参照图16，说明ECU初始密钥的共享方法的例2。

[0199] (步骤S611)第二ECU1020向第一ECU1010发送自己的ECU标识符ECU_ID_S。该发送的时刻例如是第二ECU1020搭载于机动车1001后初次通电时等。

[0200] (步骤S612)第一ECU1010向HSM1012提供从第二ECU1020接收到的ECU标识符ECU_ID_S。HSM1012使用该ECU标识符ECU_ID_S和密钥存储部1013中存储的第一主密钥MASTER_KEY1，生成第一值。该HSM1012的第一值生成方法与上述的图14所示的写入装置301-1的第一值生成方法相同。

[0201] (步骤S613)第一ECU1010向SIM1052发送HSM1012生成的第一值。此时，第一ECU1010可以向SIM1052发送第一值与第二ECU1020的ECU标识符ECU_ID_S的组。

[0202] (步骤S614)SIM1052使用从第一ECU1010接收到的第一值和密钥存储部1053中存储的第二主密钥MASTER_KEY2，生成第二ECU1020的ECU初始密钥Key_S。该SIM1052的ECU初始密钥生成方法与上述的图14所示的写入装置301-2的ECU初始密钥生成方法相同。

[0203] (步骤S615)SIM1052将生成的ECU初始密钥Key_S发送给第一ECU1010。此时，SIM1052可以向第一ECU1010发送ECU初始密钥Key_S与第二ECU1020的ECU标识符ECU_ID_S的组。

[0204] 第一ECU1010向HSM1012提供从SIM1052接收到的第二ECU1020的ECU初始密钥Key_S。HSM1012的密钥存储部1013将该第二ECU1020的ECU初始密钥Key_S与第二ECU1020的ECU标识符ECU_ID_S关联地存储。由此，在第一ECU1010和第二ECU1020之间共享相同的ECU初始密钥Key_S。该共享的ECU初始密钥Key_S例如用于在第一ECU1010的HSM1012和第二ECU1020

的SHE1022之间交换的数据的加密等。

[0205] 第一ECU1010中，与第二ECU1020的ECU初始密钥Key_S进行关联的第二ECU1020的ECU标识符ECU_ID_S可以将在步骤S611中从第二ECU1020接收到的ECU标识符ECU_ID_S进行记录，或者，也可以使用在步骤S615中从SIM1052接收到的ECU初始密钥Key_S与第二ECU1020的ECU标识符ECU_ID_S的组中包括的ECU标识符ECU_ID_S。

[0206] 上述的ECU初始密钥的共享方法的例2中，HSM1012是第一值生成装置的例。另外，SIM1052是初始密钥生成装置的例。另外，HSM1012和SIM1052是密钥管理系统的例。

[0207] 需要说明的是，上述的ECU初始密钥的共享方法的例2中，HSM1012可以不接收与已经接收到的用于生成第一值的ECU标识符ECU_ID_S相同的ECU标识符ECU_ID_S。例如，HSM1012可以不接收与和密钥存储部1013中存储的ECU初始密钥Key_S进行关联的ECU标识符ECU_ID_S相同的ECU标识符ECU_ID_S。由此，攻击者即使获取ECU标识符ECU_ID_S，也不能利用HSM1012非法地生成第一值，因此能够防止第一值的非法获取。SIM1052可以不接收与已经用于生成ECU初始密钥Key_S的第一值相同的第一值。由此，攻击者即使获取第一值，也不能利用SIM1052非法地生成ECU初始密钥Key_S，因此能够防止ECU初始密钥Key_S的非法获取。

[0208] [ECU初始密钥的共享方法的例3]

[0209] 参照图17说明ECU初始密钥的共享方法的例3。图17是示出第六实施方式的ECU初始密钥的共享方法(例3)的顺序图。

[0210] 与上述的ECU初始密钥的共享方法的例2同样地，本ECU初始密钥的共享方法的例3将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同标准的安全元件中。具体而言，图17中，通信模块1051的SIM1052将第一主密钥MASTER_KEY1存储在密钥存储部1053中，第一ECU1010的HSM1012将第二主密钥MASTER_KEY2存储在密钥存储部1013中。在制造SIM1052时等，第一主密钥MASTER_KEY1被安全地存储在该SIM1052中。在制造HSM1012时等，第二主密钥MASTER_KEY2被安全地存储在HSM1012中。除该主密钥的分散管理相关的点以外，通信模块1051的SIM1052、第一ECU1010的HSM1012以及第二ECU1020的SHE1022与图15所示的ECU初始密钥的共享方法的例1的结构相同。下面，参照图17，说明ECU初始密钥的共享方法的例3。

[0211] (步骤S621)第二ECU1020经由第一ECU1010向SIM1052提供自己的ECU标识符ECU_ID_S。该提供的时刻例如是第二ECU1020搭载于机动车1001后初次通电时等。

[0212] (步骤S622)SIM1052使用从第二ECU1020提供的ECU标识符ECU_ID_S和密钥存储部1053中存储的第一主密钥MASTER_KEY1，生成第一值。该SIM1052的第一值生成方法与上述的图14所示的写入装置301-1的第一值生成方法相同。

[0213] (步骤S623)SIM1052将生成的第一值发送给第一ECU1010。此时，SIM1052可以向第一ECU1010发送第一值与第二ECU1020的ECU标识符ECU_ID_S的组。

[0214] (步骤S624)第一ECU1010向HSM1012提供从SIM1052接收到的第一值。HSM1012使用该第一值和密钥存储部1013中存储的第二主密钥MASTER_KEY2，生成第二ECU1020的ECU初始密钥Key_S。该HSM1012的ECU初始密钥生成方法与上述的图14所示的写入装置301-2的ECU初始密钥生成方法相同。

[0215] HSM1012的密钥存储部1013将生成的第二ECU1020的ECU初始密钥Key_S与第二

ECU1020的ECU标识符ECU_ID_S关联地存储。由此，在第一ECU1010与第二ECU1020之间共享相同的ECU初始密钥Key_S。该共享的ECU初始密钥Key_S例如用于在第一ECU1010的HSM1012与第二ECU1020的SHE1022之间交换的数据的加密等。

[0216] 第一ECU1010中，与第二ECU1020的ECU初始密钥Key_S进行关联的第二ECU1020的ECU标识符ECU_ID_S可以在步骤S621中传输第二ECU1020的ECU标识符ECU_ID_S时记录该ECU标识符ECU_ID_S，或者，可以使用在步骤S623中从SIM1052接收的第一值与第二ECU1020的ECU标识符ECU_ID_S的组中包括的ECU标识符ECU_ID_S。

[0217] 上述的ECU初始密钥的共享方法的例3中，SIM1052是第一值生成装置的例。另外，HSM1012是初始密钥生成装置的例。另外，SIM1052和HSM1012是密钥管理系统的例。

[0218] 需要说明的是，上述的ECU初始密钥的共享方法的例3中，SIM1052可以不接收与已经接收到的用于生成第一值的ECU标识符ECU_ID_S相同的ECU标识符ECU_ID_S。由此，攻击者即使获取ECU标识符ECU_ID_S，也不能利用SIM1052非法地生成第一值，因此能够防止第一值的非法获取。

[0219] HSM1012可以不接收与已经接收到的用于提供给SIM1052的ECU标识符ECU_ID_S相同的ECU标识符ECU_ID_S。例如，HSM1012可以不接收与和密钥存储部1013中存储的ECU初始密钥Key_S进行关联的ECU标识符ECU_ID_S相同的ECU标识符ECU_ID_S。由此，攻击者即使获取ECU标识符ECU_ID_S，也不能利用HSM1012向SIM1052提供ECU标识符ECU_ID_S且非法地生成第一值，因此能够防止第一值的非法获取。

[0220] HSM1012可以不接收与已经用于生成ECU初始密钥Key_S的第一值相同的第一值。由此，攻击者即使获取第一值，也不能利用HSM1012非法地生成ECU初始密钥Key_S，因此能够防止ECU初始密钥Key_S的非法获取。

[0221] 上述的ECU初始密钥的共享方法的例2及例3中，机动车1001中，第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同的安全元件中。由此，与将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2一同保管在相同的安全元件中的情况相比，分散保管第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2可以提高主密钥的安全性。

[0222] 而且，上述的ECU初始密钥的共享方法的例2及例3中，机动车1001中，第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同标准的安全元件中。由此，与将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在相同标准的安全元件中的情况相比，提高了主密钥的安全性。下面说明这一效果。

[0223] 在将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同的但标准相同的安全元件中的情况下，对于相同标准的一个安全元件的破解成功则一个主密钥例如第一主密钥MASTER_KEY1发生泄露。结果，根据相同的破解方法，对于相同标准的另一个安全元件的破解成功则另一个第二主密钥MASTER_KEY2也可能发生泄露。

[0224] 对此，根据ECU初始密钥的共享方法的例2及例3，将第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2分别保管在不同标准的安全元件中。由此，即使对于一个标准的安全元件的破解成功而一个主密钥例如第一主密钥MASTER_KEY1发生了泄露，根据该相同的破解方法，对于另一个标准的安全元件的破解也会失败，能够防止另一个第二主密钥MASTER_KEY2的泄露。由此，能够进一步提高ECU初始密钥的安全性。

[0225] 上述的图16所示的ECU初始密钥的共享方法的例2及图17所示的ECU初始密钥的共

享方法的例3中，作为分散保管第一主密钥MASTER_KEY1和第二主密钥MASTER_KEY2的安全元件，使用了SIM和HSM。SIM和HSM的标准不同。具体而言，SIM和HSM的防篡改性的技术标准不同。作为防篡改性的技术，例如，举出用于信息保护的硬件技术。作为用于信息保护的硬件技术，例如，举出通过对安全元件实施物理或电破解方法，删除该安全元件内部的信息或者破坏该安全元件内部的线路或者该安全元件的动作停止的技术。另外，作为用于信息保护的硬件技术，举出使通过测定来自安全元件的泄露电磁波的破解困难化的技术等。

[0226] 本实施方式中，作为分散保管多个主密钥的多个安全元件，使用标准不同的多个安全元件。另外，作为分散保管多个主密钥的多个安全元件，也可以使用防篡改性的技术标准不同的多个安全元件。作为安全元件，例如，举出SIM、SIM的一种的eSIM、HSM、TPM以及SHE等。

[0227] [第六实施方式的变形例1]

[0228] 上述的第六实施方式中，在机动车1001内部生成ECU初始密钥，但与上述的第二实施方式同样地，机动车外部的管理服务器装置也可以生成ECU初始密钥。

[0229] 机动车外部的管理服务器装置保管多个主密钥。从机动车通过无线向管理服务器装置发送该机动车的ECU的ECU标识符。管理服务器装置使用该ECU的ECU标识符和自身保管的多个主密钥生成该ECU的ECU初始密钥，并通过无线将生成的ECU初始密钥发送给该机动车。

[0230] [第六实施方式的变形例2]

[0231] 另外，可以将多个主密钥分散保管在机动车内部的安全元件例如SIM和机动车外部的管理服务器装置中。SIM和管理服务器装置中的任一个使用自己的主密钥和机动车的ECU的ECU标识符生成第一值，并将生成的第一值通过无线发送给SIM和管理服务器装置中的另一个。SIM和管理服务器装置中的该另一个使用自己的主密钥和该第一值生成该ECU的ECU初始密钥。在该另一个是管理服务器装置的情况下，将生成的ECU初始密钥从管理服务器装置通过无线发送给机动车。

[0232] [第六实施方式的变形例3]

[0233] 图18是示出第六实施方式的机动车1001的变形例的框图。图18中，对与图13的各部对应的部分标记相同的符号，并省略其说明。图18所示的变形例中，可以将维护工具(maintenance tool)1200连接到诊断端口1060。第一ECU1010和连接到诊断端口1060的维护工具1200经由诊断端口1060交换数据。维护工具1200可以具有连接到OBD端口的传统的诊断终端的功能。

[0234] 维护工具1200具有控制模块1201。控制模块1201具有IC(Integrated Circuit;集成电路)芯片1202。IC芯片1202具有存储密钥的密钥存储部1203。IC芯片1202具有防篡改性。IC芯片1202是安全元件的例。IC芯片1202是计算机的一种，通过计算机程序实现期望的功能。

[0235] 图18所示的变形例中，IC芯片1202与图13所示的SIM1052对应，密钥存储部1023与图13所示的密钥存储部1053对应。图18所示的变形例中，图15所示的ECU初始密钥的共享方法的例1、图16所示的ECU初始密钥的共享方法的例2、以及图17所示的ECU初始密钥的共享方法的例3中，IC芯片1202代替SIM1052，密钥存储部1023代替密钥存储部1053。

[0236] 需要说明的是，上述的实施方式中，举出了机动车作为车辆的例子，但也可以适用

于机动自行车、铁路车辆等机动车以外的其他车辆。

[0237] 另外，可以在计算机可读的记录介质中记录用于实现上述的管理装置10或10a执行的管理方法的各步骤的计算机程序，或者用于实现上述的各装置执行的各步骤的计算机程序，使计算机系统读取并执行在该记录介质中记录的程序。需要说明的是，此处所说的“计算机系统”可以包括OS或外围设备等硬件。

[0238] 另外，“计算机可读的记录介质”是指软盘、光磁盘、ROM、闪存等可写非易失性存储器、DVD(Digital Versatile Disc;数字多功能光盘)等可移动介质、计算机系统内置的硬盘等存储装置。

[0239] 此外，“计算机可读的记录介质”也包括如在经由互联网等的网络、电话线路等通信线路发送程序时作为服务器、客户端的计算机系统内部的易失性存储器(例如，DRAM(Dynamic Random Access Memory;动态随机存取存储器))那样一定时间保存程序的介质。

[0240] 另外，上述程序可以被从将该程序存储在存储装置等中的计算机系统，经由传输介质或者通过传输介质中的传输波向其他计算机系统传输。此处，传输程序的“传输介质”是指如互联网等网络(通信网)、电话线路等通信线路(通信线)这样的具有传输信息的功能的介质。

[0241] 另外，上述程序可以用于实现所述功能的一部分。

[0242] 此外，可以是通过与已经记录在计算机系统中的程序的组合来实现所述功能的所谓的差分文件(差分程序)。

[0243] 附图标记说明

[0244] 1、1001:机动车

[0245] 2:无线通信网络

[0246] 3:无线通信线路

[0247] 4:通信线路

[0248] 10、10a:管理装置

[0249] 11:控制部

[0250] 12:CAN接口

[0251] 13:无线通信部

[0252] 20:安全元件

[0253] 20a、1052:SIM(安全元件)

[0254] 21:密钥生成部

[0255] 22、1013、1023、1053、1203:密钥存储部

[0256] 23:验证部

[0257] 24:加密处理部

[0258] 31:主密钥存储部

[0259] 32:ECU初始密钥存储部

[0260] 80:管理服务器装置

[0261] 1002:车载计算机系统

[0262] 1010:第一ECU

[0263] 1011、1021:主运算器

[0264] 1012:HSM

[0265] 1020:第二ECU

[0266] 1022:SHE

[0267] 1030:CAN

[0268] 1040:信息娱乐设备

[0269] 1050:TCU

[0270] 1051:通信模块

[0271] 1060:诊断端口

[0272] 1200:维护工具

[0273] 1201:控制模块

[0274] 1202:IC芯片

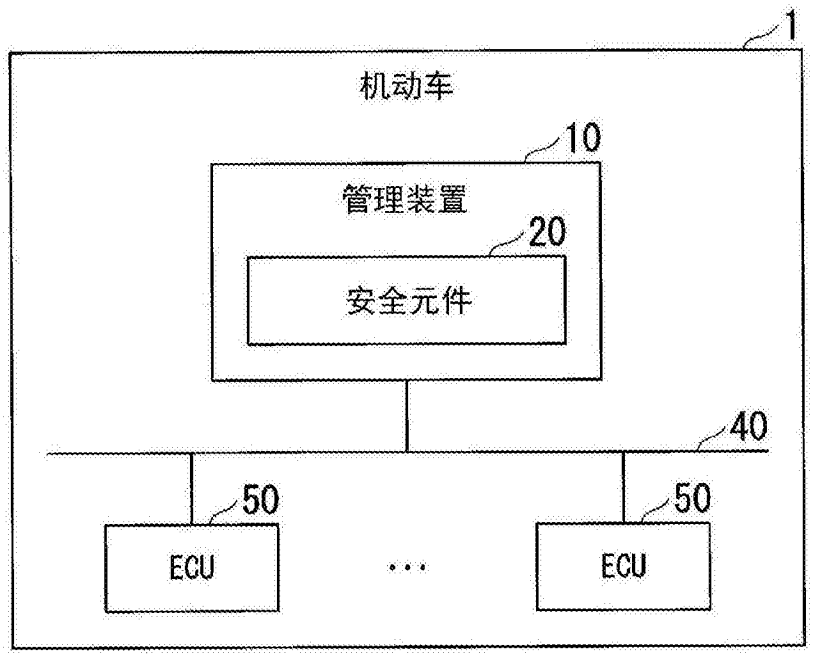

1
机动车
10
管理装置
20
安全元件
40
50
50
ECU
…
ECU

图1

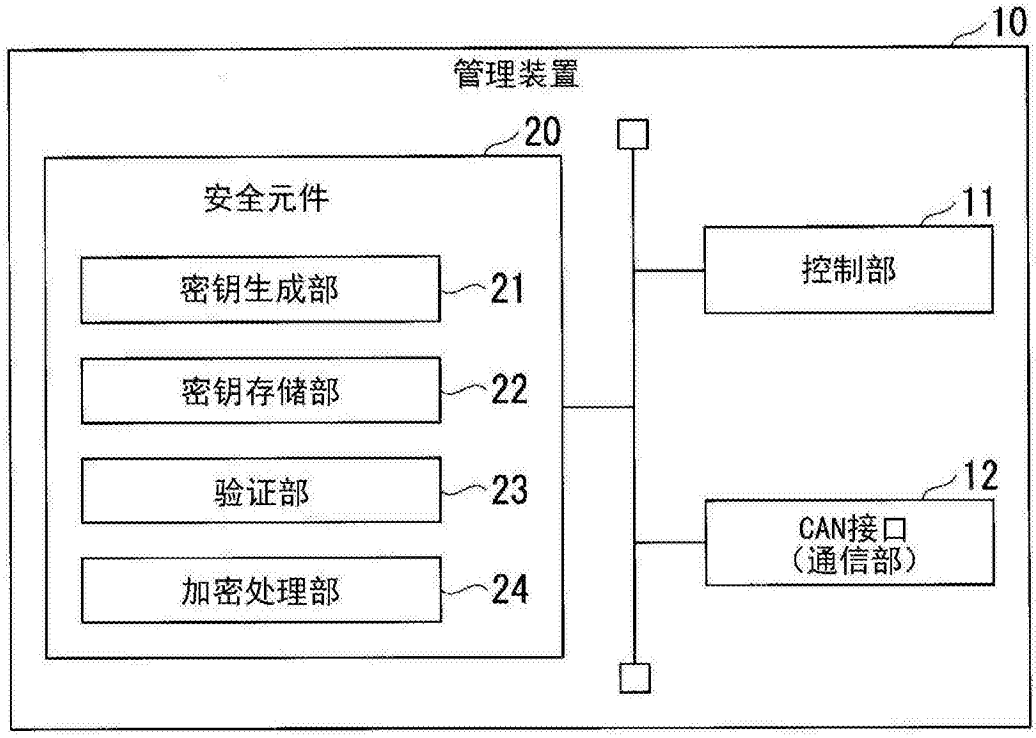

10
管理装置
20
安全元件
密钥生成部
21
密钥存储部
22
验证部
23
加密处理部
24
11
控制部
12
CAN接口
（通信部）

图2

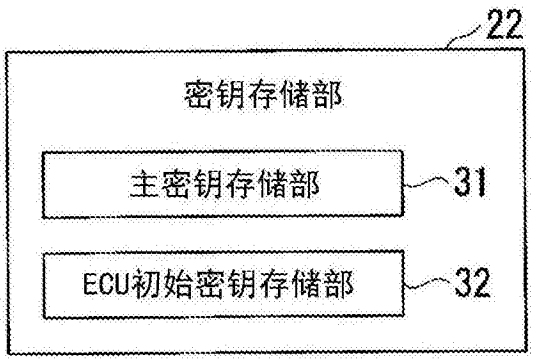

22
密钥存储部
主密钥存储部
31
ECU初始密钥存储部
32

图3

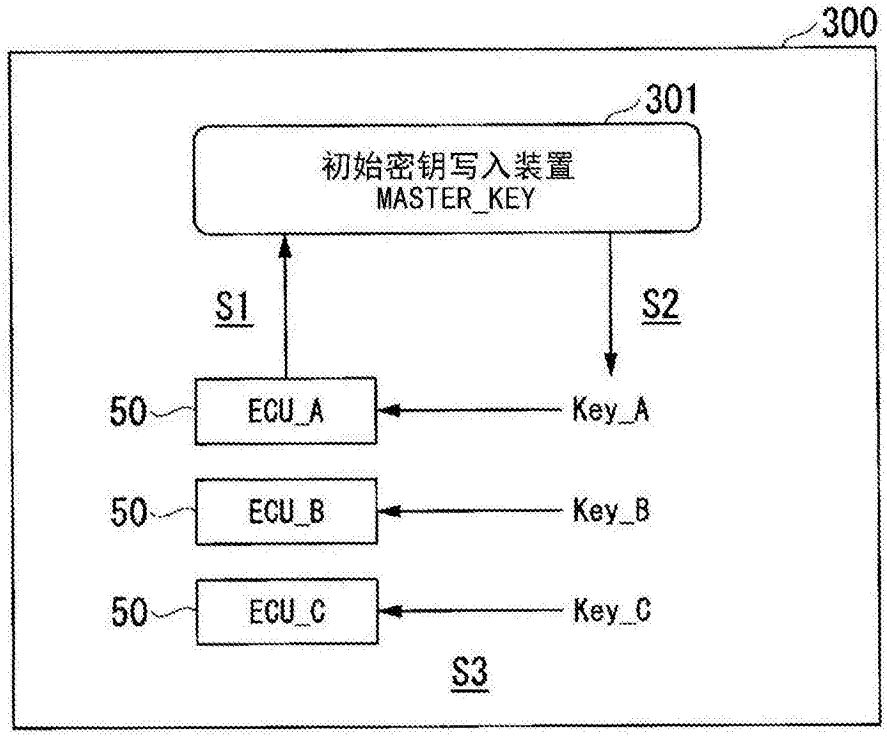

300
301
初始密钥写入装置
MASTER_KEY
S1
S2
50
ECU_A
Key_A
50
ECU_B
Key_B
50
ECU_C
Key_C
S3

图4

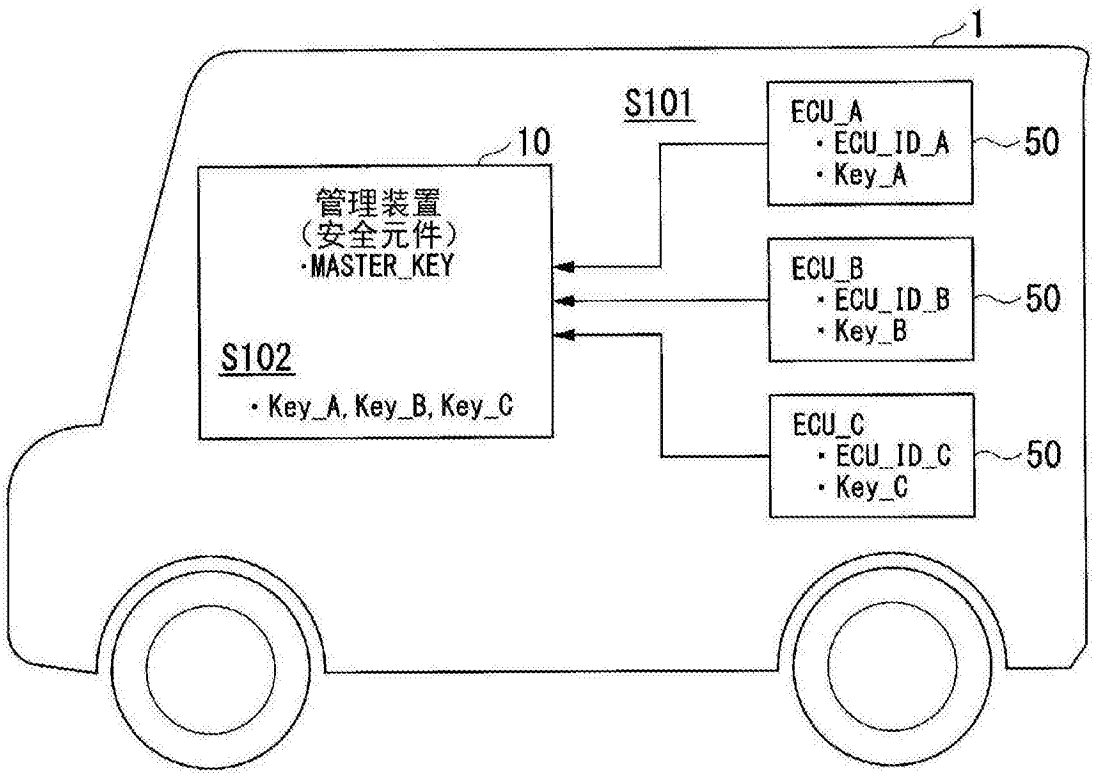

1
S101
10
管理装置
（安全元件）
·MASTER_KEY
S102
· Key_A, Key_B, Key_C
ECU_A
· ECU_ID_A
· Key_A
50
ECU_B
· ECU_ID_B
· Key_B
50
ECU_C
· ECU_ID_C
· Key_C
50

图5

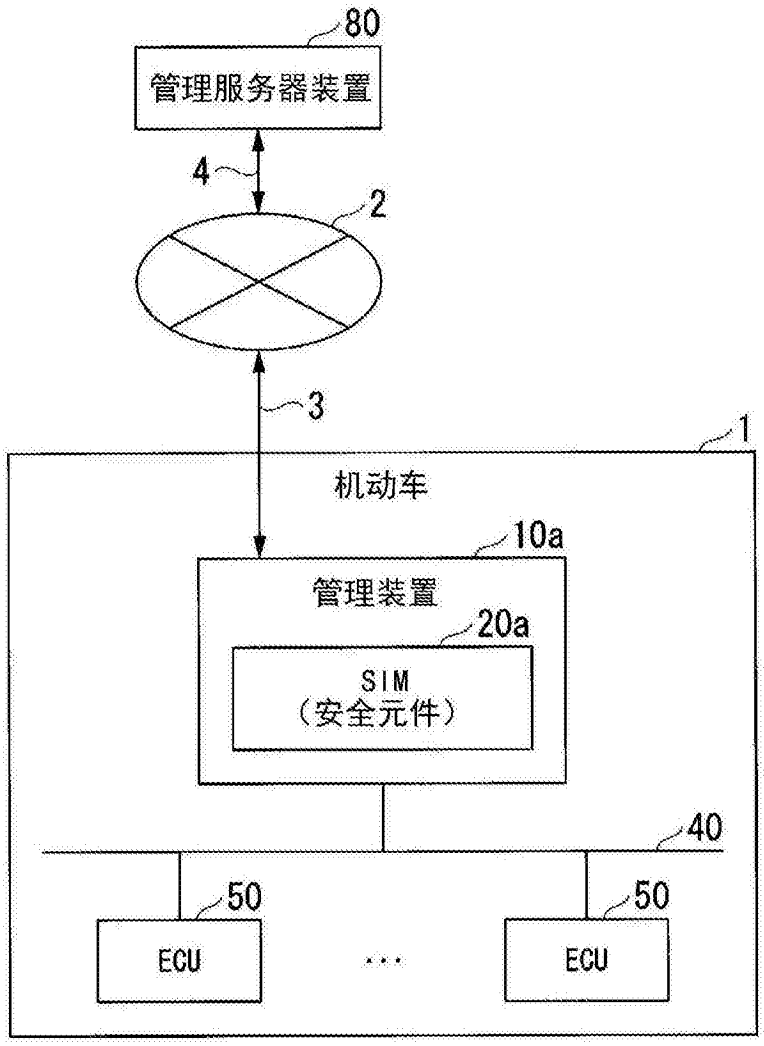


图6

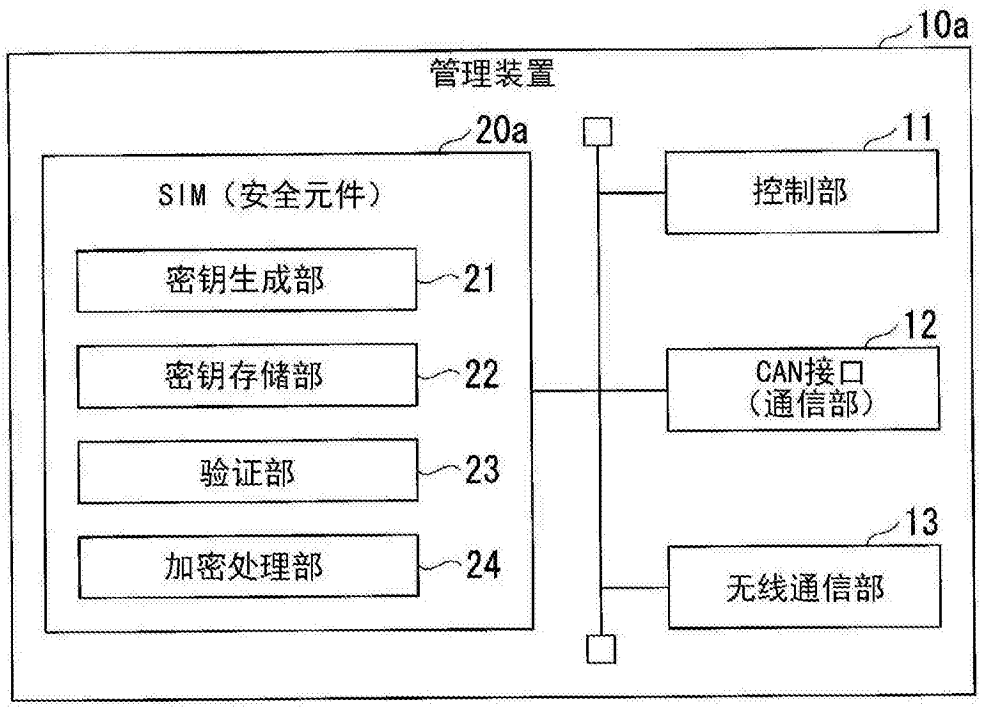

10a
管理装置
20a
SIM（安全元件）
密钥生成部
21
密钥存储部
22
验证部
23
加密处理部
24
11
控制部
12
CAN接口
（通信部）
13
无线通信部

图7

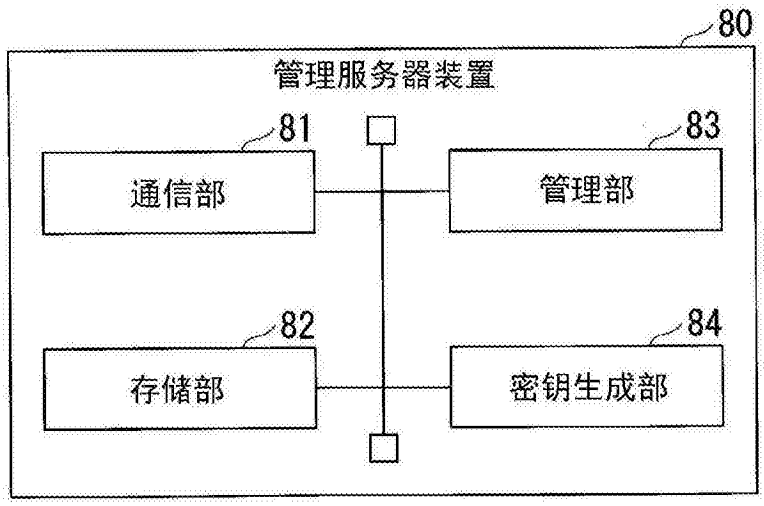

80
管理服务器装置
81
通信部
83
管理部
82
存储部
84
密钥生成部

图8

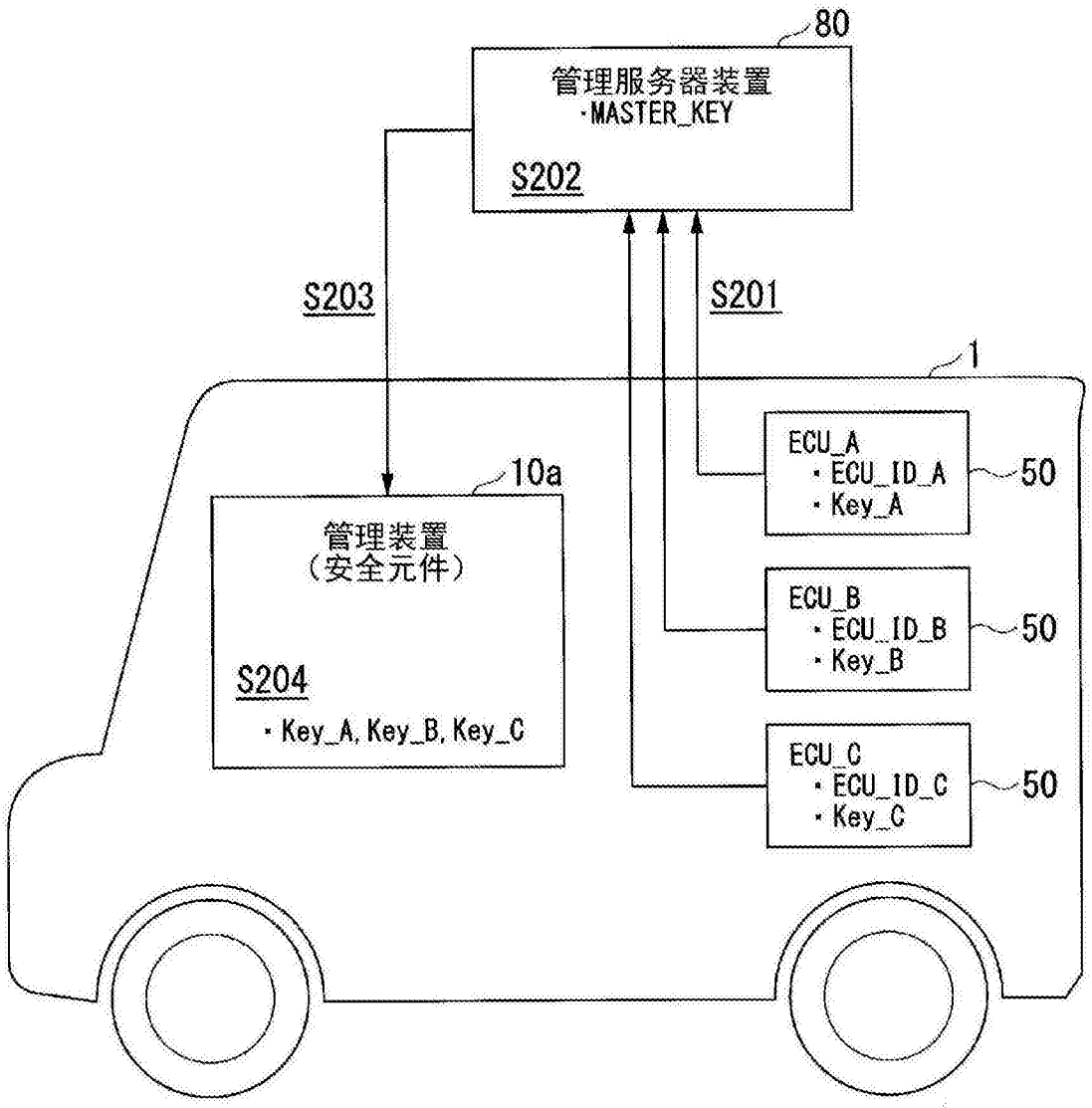

80
管理服务器装置
·MASTER_KEY
S202
S203
S201
1
ECU_A
· ECU_ID_A
· Key_A
50
10a
管理装置
（安全元件）
S204
· Key_A, Key_B, Key_C
ECU_B
· ECU_ID_B
· Key_B
50
ECU_C
· ECU_ID_C
· Key_C
50

图9

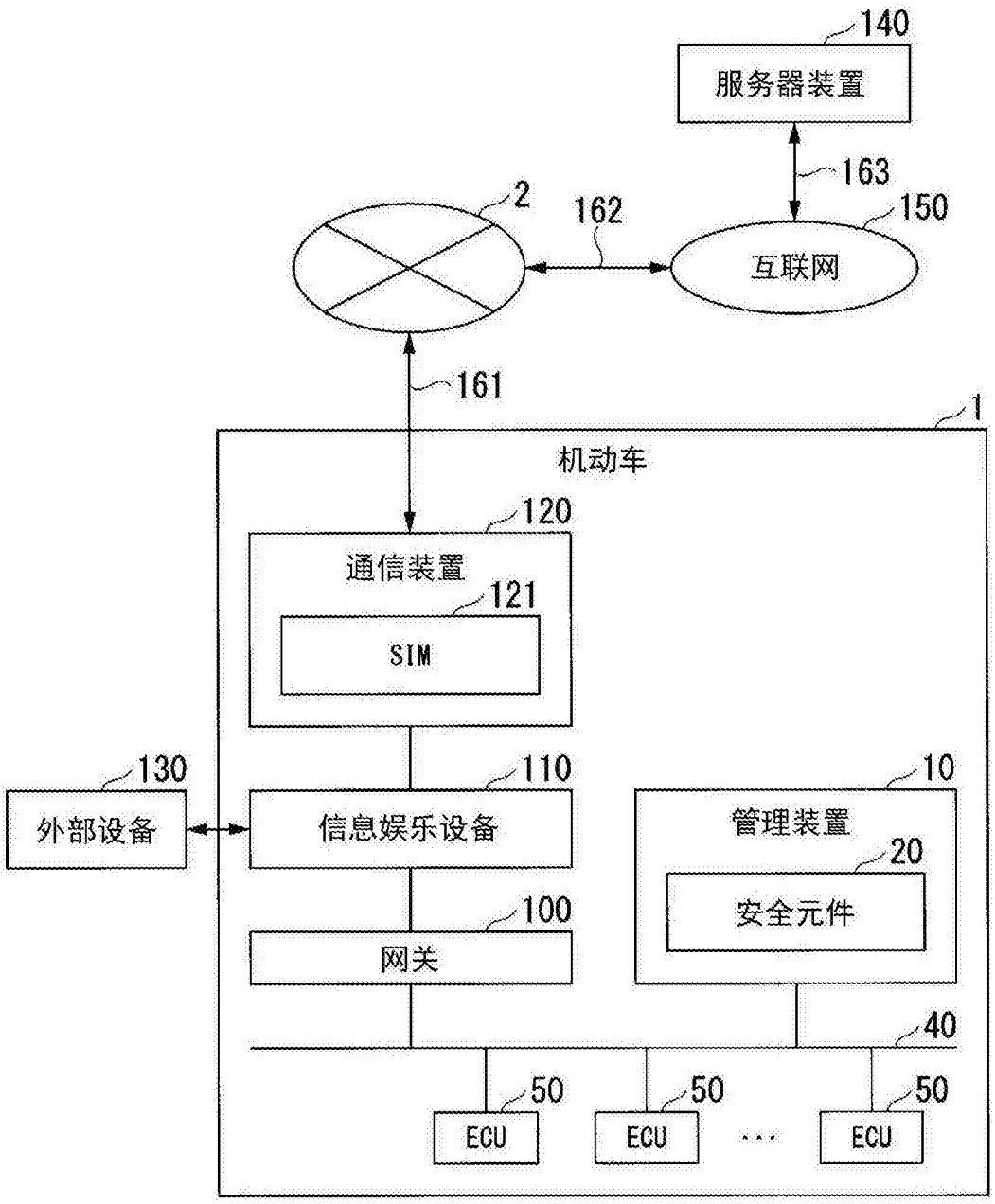

140
服务器装置
163
2
162
150
互联网
161
1
机动车
120
通信装置
121
SIM
130
外部设备
110
信息娱乐设备
10
管理装置
20
安全元件
100
网关
40
50
50
50
ECU
ECU
ECU

图10

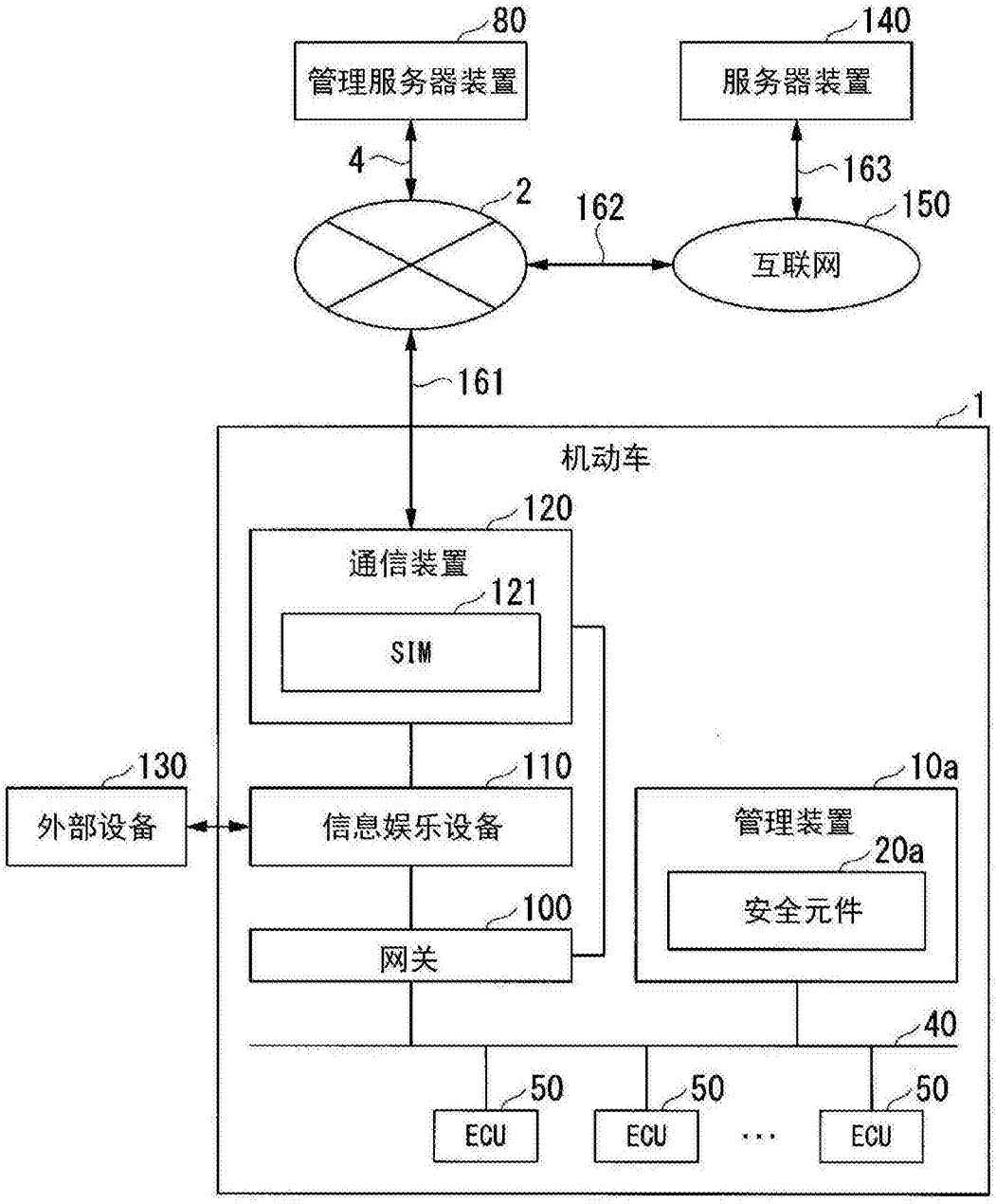

80
管理服务器装置
140
服务器装置
4
2
162
163
150
互联网
161
1
机动车
120
通信装置
121
SIM
130
外部设备
110
信息娱乐设备
10a
管理装置
20a
安全元件
100
网关
40
50
ECU
50
ECU
50
ECU

图11

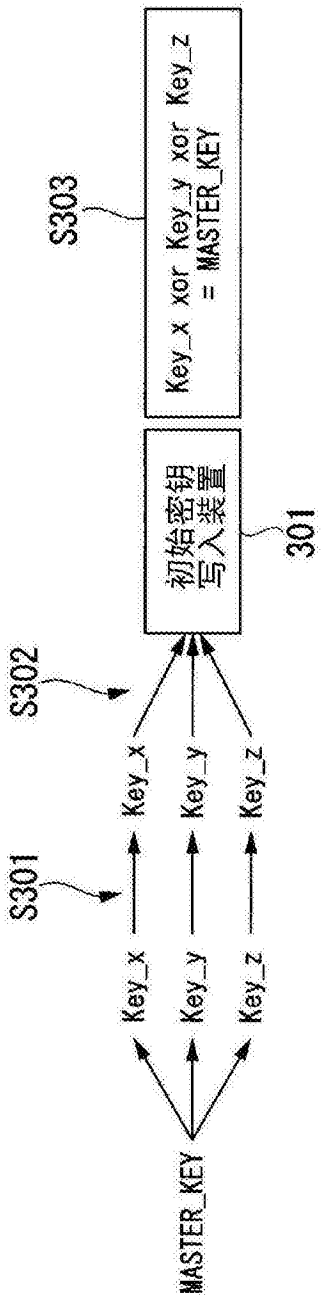

S303
Key_x xor Key_y xor Key_z
= MASTER_KEY
初始密钥
写入装置
301
S302
Key_x
Key_y
Key_z
S301
Key_x
Key_y
Key_z
MASTER_KEY

图12

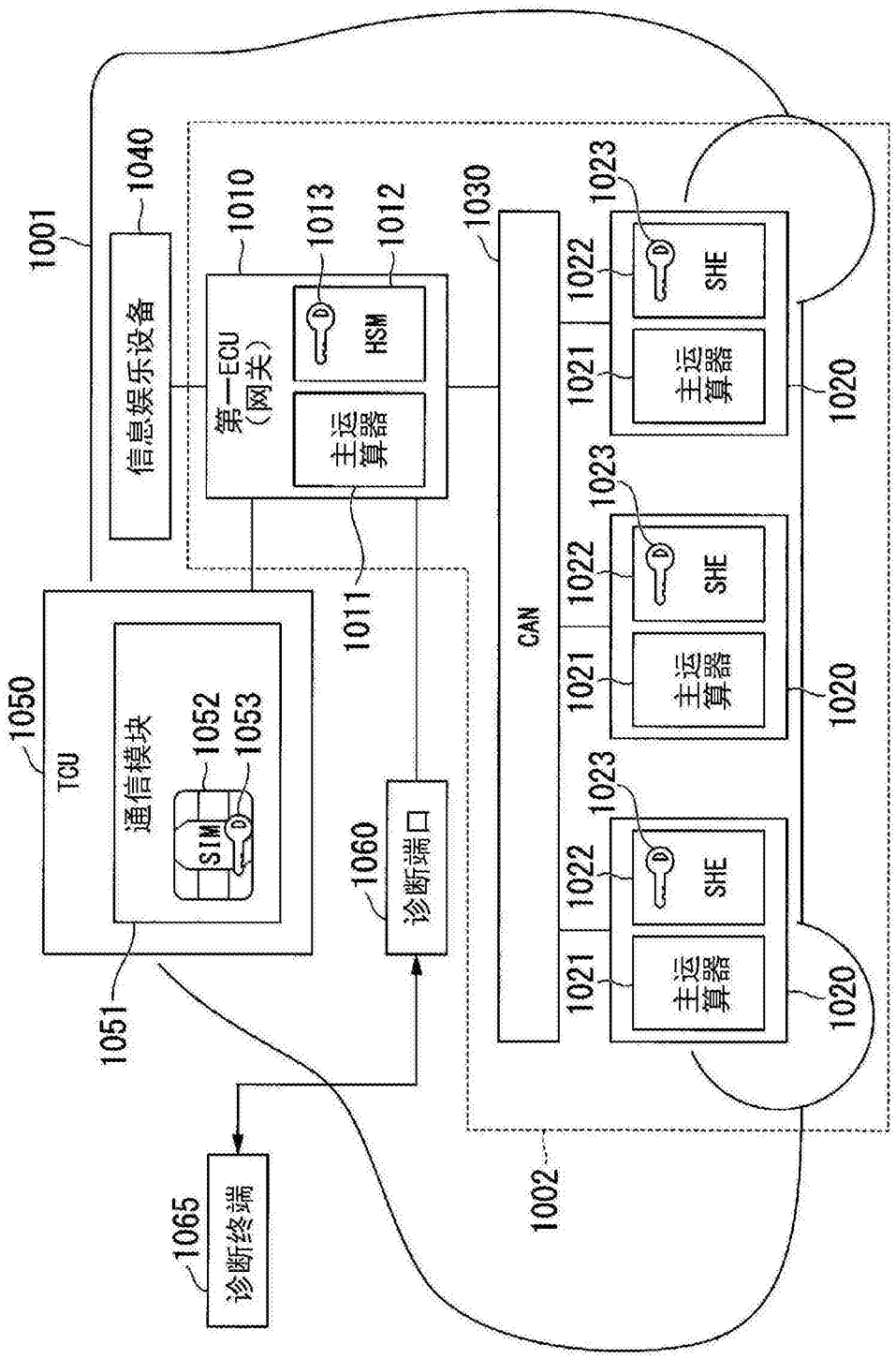

1001
1040
信息娱乐设备
1010
第一ECU
（网关）
1013
HSM
1012
主运算器
1011
1030
CAN
1023
SHE
1022
1021
主运算器
1020
1050
TCU
通信模块
1052
1053
SIM
1051
1060
诊断端口
1065
诊断终端
1002

图13

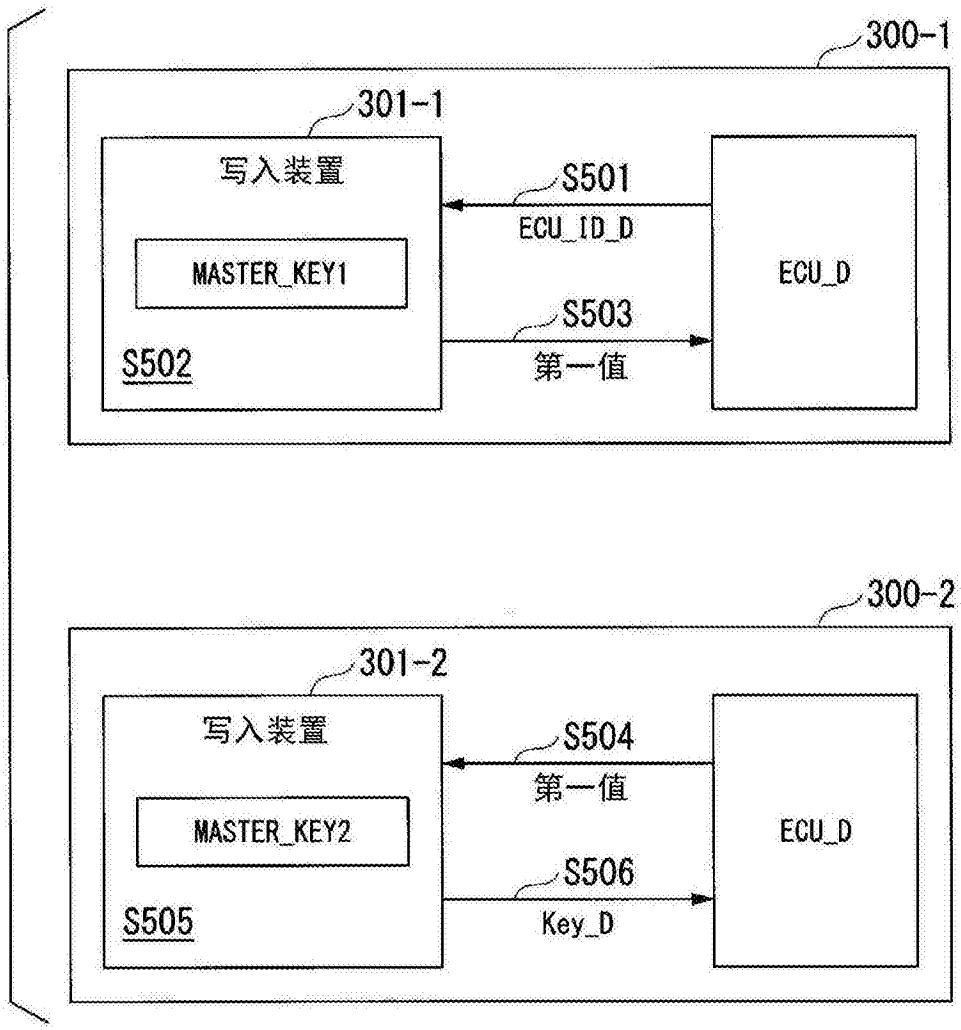

300-1
301-1
写入装置
MASTER_KEY1
S502
S501
ECU_ID_D
S503
第一值
ECU_D
300-2
301-2
写入装置
MASTER_KEY2
S505
S504
第一值
S506
Key_D
ECU_D

图14

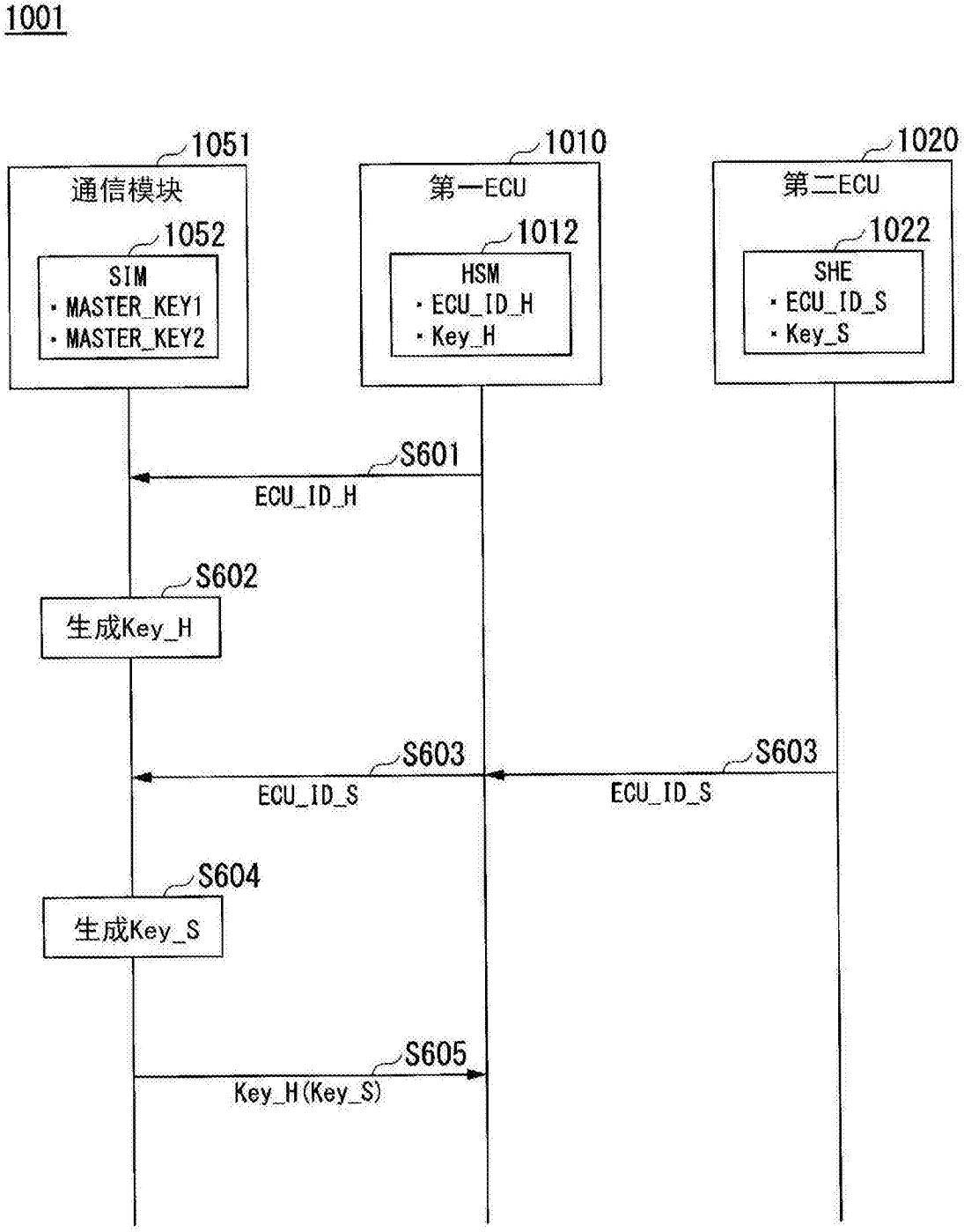

1001
1051
通信模块
1052
SIM
· MASTER_KEY1
· MASTER_KEY2
1010
第一ECU
1012
HSM
· ECU_ID_H
· Key_H
1020
第二ECU
1022
SHE
· ECU_ID_S
· Key_S
S601
ECU_ID_H
S602
生成Key_H
S603
ECU_ID_S
S603
ECU_ID_S
S604
生成Key_S
S605
Key_H(Key_S)

图15

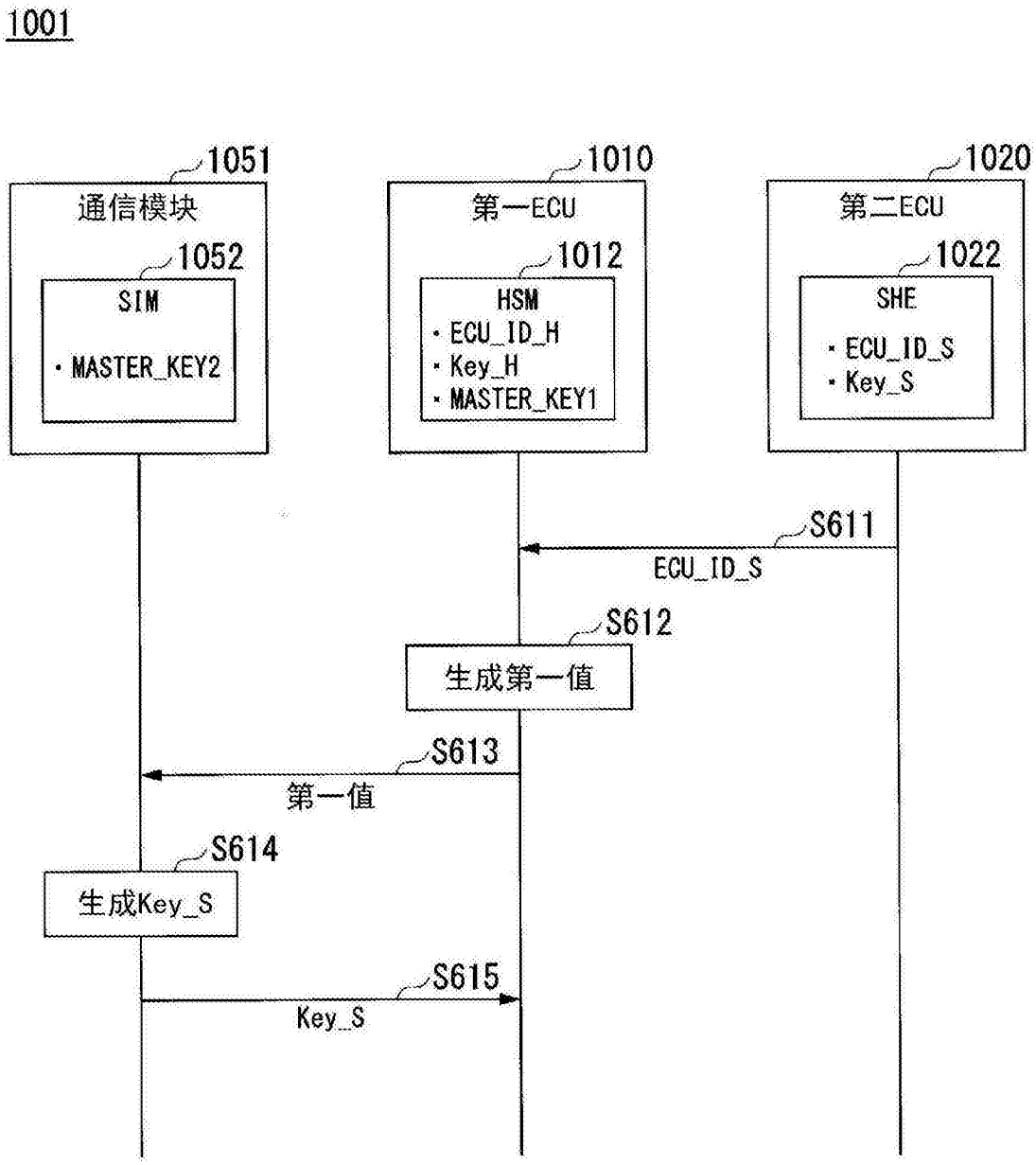

1001
1051
通信模块
1052
SIM
· MASTER_KEY2
1010
第一ECU
1012
HSM
· ECU_ID_H
· Key_H
· MASTER_KEY1
1020
第二ECU
1022
SHE
· ECU_ID_S
· Key_S
S611
ECU_ID_S
S612
生成第一值
S613
第一值
S614
生成Key_S
S615
Key_S

图16

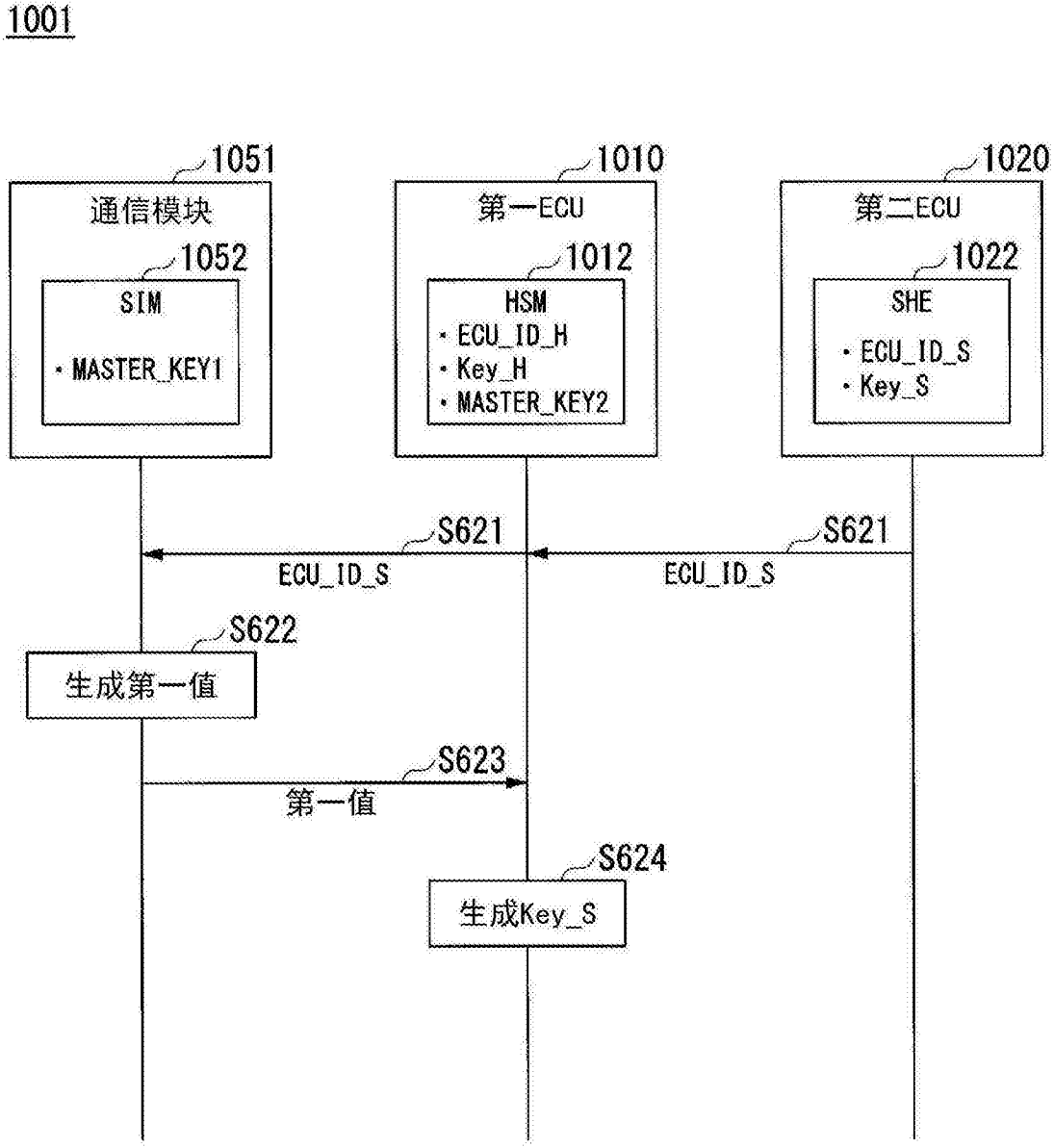

1001
1051
通信模块
1052
SIM
· MASTER_KEY1
1010
第一ECU
1012
HSM
· ECU_ID_H
· Key_H
· MASTER_KEY2
1020
第二ECU
1022
SHE
· ECU_ID_S
· Key_S
S621
ECU_ID_S
S621
ECU_ID_S
S622
生成第一值
S623
第一值
S624
生成Key_S

图17

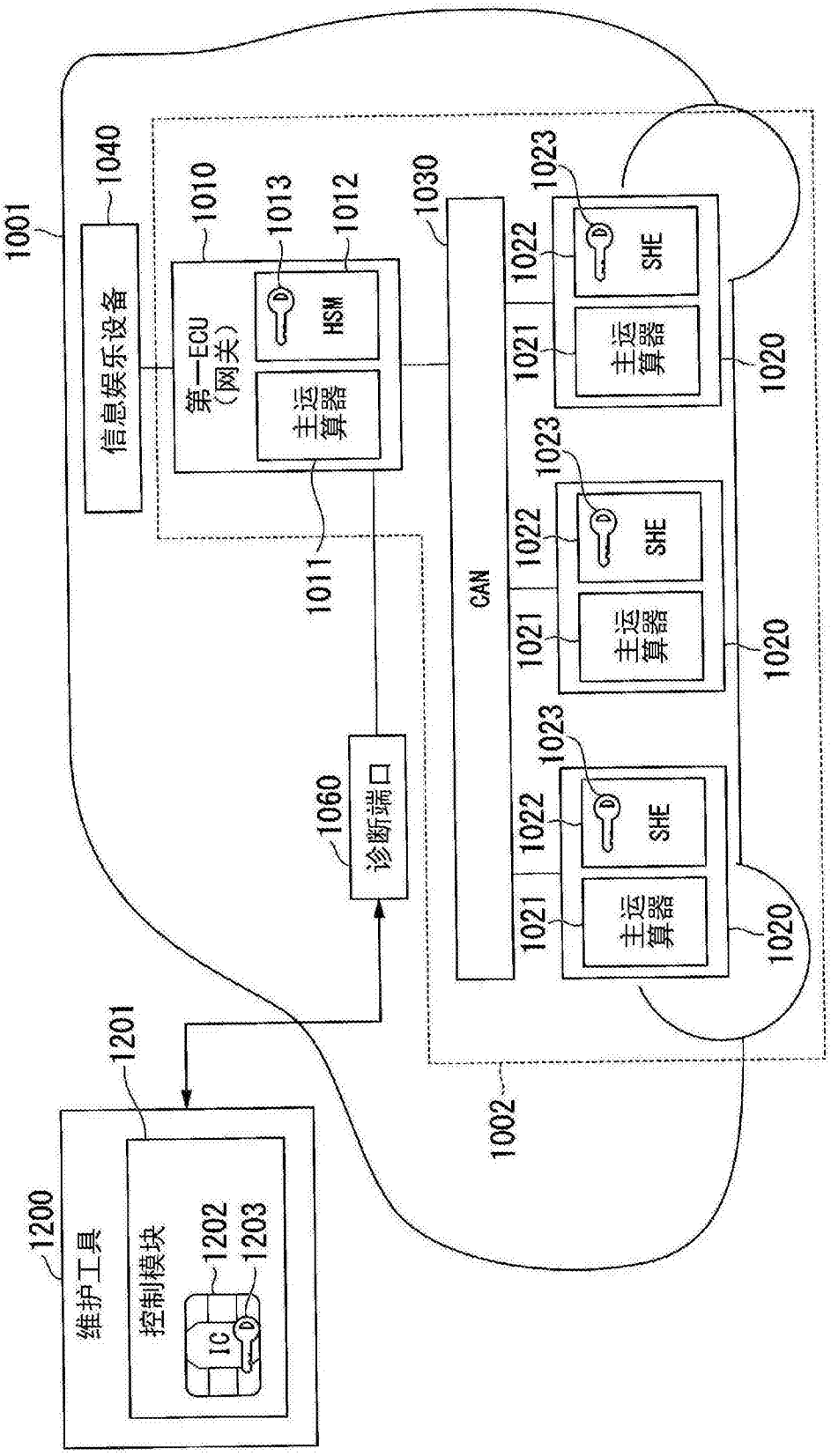

1001
1040
信息娱乐设备
1010
第一ECU（网关）
1013
HSM
1012
主运算器
1011
1030
CAN
1023
SHE
1022
1021
主运算器
1020
1060
诊断端口
1002
1200
维护工具
1201
控制模块
1202
1203
IC

图18