(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 107683583 B
(45)授权公告日 2020.12.11

(21)申请号 201680033856.6
(22)申请日 2016.03.14
(65)同一申请的已公布的文献号
申请公布号 CN 107683583 A
(43)申请公布日 2018.02.09
(30)优先权数据
2015-130315 2015.06.29 JP
(85)PCT国际申请进入国家阶段日
2017.12.08
(86)PCT国际申请的申请数据
PCT/JP2016/057939 2016.03.14
(87)PCT国际申请的公布数据
WO2017/002405 JA 2017.01.05
(73)专利权人 歌乐株式会社
地址 日本埼玉县
(72)发明人 伯田惠辅 森田伸义 安藤英里子 大和田彻 萱岛信
(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 范胜杰 赵宇
(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/44(2006.01)
(56)对比文件
US 2009119657 A1,2009.05.07
CN 103200165 A,2013.07.10
US 2015180840 A1,2015.06.25
JP 2015076018 A,2015.04.20
WO 2013005730 A1,2013.01.10
WO 2009147734 A1,2009.12.10
审查员 傅琦

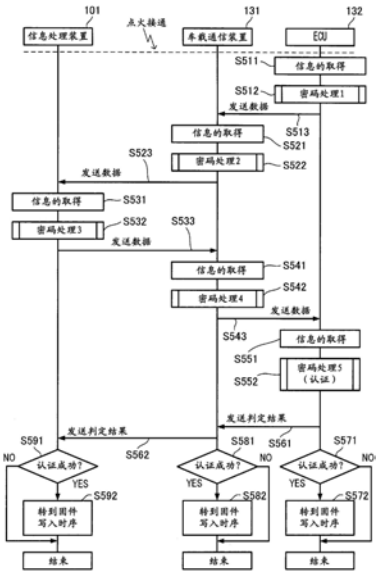
权利要求书3页 说明书16页 附图14页

(54)发明名称

车载信息通信系统以及认证方法

(57)摘要

车载信息通信系统由车载通信装置、车载的电子控制装置以及不是车载的信息处理装置构成。电子控制装置具备电子控制装置存储部、消息生成部、MAC生成部以及经由车载通信装置将消息以及MAC发送给信息处理装置的电子控制装置通信部。信息处理装置具备信息处理装置存储部、消息认证编码验证部、响应编码生成部以及将响应编码经由车载通信装置发送给电子控制装置的信息处理装置通信部。电子控制装置还具备响应编码验证部。



CN 107683583 B

1.一种车载信息通信系统，由搭载于车辆的车载通信装置、电子控制装置以及未搭载于车辆的信息处理装置构成，其特征在于，

上述电子控制装置具备：

电子控制装置存储部，其存储事先与所述信息处理装置共享的通用密钥；

消息生成部，其生成用于认证的消息；

消息认证编码生成部，其使用上述通用密钥，生成与上述消息相关的消息认证编码；以及

电子控制装置通信部，其将上述消息生成部所生成的消息、以及上述消息认证编码生成部所生成的消息认证编码，经由上述车载通信装置发送给上述信息处理装置，

上述信息处理装置具备：

信息处理装置存储部，其存储上述通用密钥；

消息认证编码验证部，其使用上述通用密钥以及接收到的消息，来验证所接收到的上述消息认证编码，由此进行上述电子控制装置的认证；

响应编码生成部，其使用上述通用密钥来生成响应编码，该响应编码是通过对称密钥密码将基于接收到的上述消息的值进行加密而得的响应编码；以及

信息处理装置通信部，其在上述消息认证编码验证部的验证成功时，将上述响应编码生成部所制作的响应编码经由上述车载通信装置发送给上述电子控制装置，

上述电子控制装置还具备：

响应编码验证部，其根据上述通用密钥，验证接收到的上述响应编码，由此进行上述信息处理装置的认证，

上述车载通信装置具备：

车载通信装置存储部，其存储公开密钥密码中的公开密钥即第一公开密钥、以及公开密钥密码中的秘密密钥即第二秘密密钥；

第一署名生成部，其使用上述第二秘密密钥，生成从上述电子控制装置接收到的上述消息的电子署名即第一署名；以及

车载通信装置通信部，其将从上述电子控制装置接收到的上述消息、从上述电子控制装置接收到的上述消息认证编码、以及上述第一署名生成部所生成的上述第一署名发送给上述信息处理装置，

在上述信息处理装置的信息处理装置存储部中，还存储与上述第一公开密钥成对的第一秘密密钥、以及与第二秘密密钥成对的第二公开密钥，

上述信息处理装置具备：

第一署名验证部，其使用上述第二公开密钥以及接收到的上述消息，来验证接收到的上述第一署名，由此进行上述车载通信装置的认证；

第一随机数生成部，其生成第一随机数；

加密部，其生成加密随机数，该加密随机数是使用上述第二公开密钥对上述第一随机数生成部所生成的第一随机数进行加密而得的加密随机数；以及

第二署名生成部，其使用上述第一秘密密钥，生成上述响应编码生成部所制作的响应编码的电子署名即第二署名，

上述响应编码生成部根据接收到的上述消息、上述通用密钥以及上述第一随机数，来

生成响应编码，

信息处理装置通信部将上述第二署名发送给上述车载通信装置，

上述车载通信装置还具备：

第二署名验证部，其使用上述第一公开密钥以及从上述信息处理装置接收到的响应编码，来验证接收到的上述第二署名，由此进行上述信息处理装置的认证；以及

解密部，其使用上述第二秘密密钥，将接收到的上述加密随机数解密为解密数据，

车载通信装置通信部将从上述信息处理装置接收到的上述响应编码以及上述解密数据发送给上述电子控制装置，

上述电子控制装置的上述响应编码验证部根据上述通用密钥以及上述解密数据，来验证接收到的上述响应编码。

2.根据权利要求1所述的车载信息通信系统，其特征在于，

在搭载了该电子控制装置的车辆的点火开关被接通时，上述电子控制装置的消息生成部生成上述消息，

在上述消息生成部生成上述消息时，上述消息认证编码生成部生成上述消息认证编码，

在上述消息认证编码生成部生成上述消息认证编码时，上述电子控制装置通信部发送上述消息生成部所生成的消息以及上述消息认证编码生成部所生成的消息认证编码。

3.根据权利要求1所述的车载信息通信系统，其特征在于，

上述电子控制装置还具备：生成第二随机数的第二随机数生成部，

在上述电子控制装置存储部中还存储第一秘密信息以及第二秘密信息，

上述消息生成部使用上述第二秘密信息对上述第一秘密信息进行加密来生成加密数据，进行上述加密数据与上述第二随机数生成部所生成的第二随机数的位运算，并生成消息。

4.一种认证方法，是由搭载于车辆的车载通信装置、电子控制装置以及未搭载于车辆的信息处理装置构成的车载信息通信系统中的上述电子控制装置和上述信息处理装置的认证方法，其特征在于，

上述电子控制装置进行如下处理：

生成用于认证的消息，

使用事先与上述信息处理装置共享的通用密钥，来生成与上述消息相关的消息认证编码，

将所生成的上述消息以及所生成的上述消息认证编码经由上述车载通信装置发送给上述信息处理装置，

上述信息处理装置进行如下处理：

使用上述通用密钥以及接收到的消息，验证接收到的上述消息认证编码，由此认证上述电子控制装置，

根据接收到的上述消息以及上述通用密钥来生成响应编码，

当上述验证成功时，将所生成的上述响应编码经由上述车载通信装置发送给上述电子控制装置，

上述电子控制装置根据上述通用密钥来验证接收到的上述响应编码，由此认证上述信

息处理装置，

上述车载通信装置进行如下处理：

存储公开密钥密码中的公开密钥即第一公开密钥、以及公开密钥密码中的秘密密钥即第二秘密密钥；

使用上述第二秘密密钥，生成从上述电子控制装置接收到的上述消息的电子署名即第一署名；以及

将从上述电子控制装置接收到的上述消息、从上述电子控制装置接收到的上述消息认证编码、以及上述第一署名发送给上述信息处理装置，

在上述信息处理装置中还存储与上述第一公开密钥成对的第一秘密密钥、以及与第二秘密密钥成对的第二公开密钥，

上述信息处理装置进行如下处理：

使用上述第二公开密钥以及接收到的上述消息，来验证接收到的上述第一署名，由此进行上述车载通信装置的认证；

生成第一随机数；

生成加密随机数，该加密随机数是使用上述第二公开密钥对上述第一随机数进行加密而得的加密随机数；以及

使用上述第一秘密密钥，生成上述响应编码的电子署名即第二署名，

根据接收到的上述消息、上述通用密钥以及上述第一随机数，来生成响应编码，

将上述第二署名发送给上述车载通信装置，

上述车载通信装置还进行如下处理：

使用上述第一公开密钥以及从上述信息处理装置接收到的响应编码，来验证接收到的上述第二署名，由此进行上述信息处理装置的认证；以及

使用上述第二秘密密钥，将接收到的上述加密随机数解密为解密数据，

将从上述信息处理装置接收到的上述响应编码以及上述解密数据发送给上述电子控制装置，

上述电子控制装置根据上述通用密钥以及上述解密数据，来验证接收到的上述响应编码。

车载信息通信系统以及认证方法

技术领域

[0001] 本发明涉及车载信息通信系统以及认证方法。

背景技术

[0002] 人们认识到,随着汽车车载设备的网络化和车载软件的增加,即使在汽车的领域也需要引入信息安全技术。特别是从车外的信息处理装置通过无线发送并更新电子控制单元(ECU:Electric Control Unit)的固件的服务也正在开始,引入上述固件更新的安全技术的必要性提高。

[0003] 专利文献1中公开以下发明:在由ECU、中心以及存在于连接ECU和中心的通信路径上的重写装置构成的通信系统中,当中心对重写装置进行认证时,则从中心向重写装置发送ECU的固件重写所需要的秘密信息。

[0004] 现有技术文献

[0005] 专利文献

[0006] 专利文献1:日本特开2004-348767号公报

发明内容

[0007] 发明要解决的课题

[0008] 在专利文献1所记载的发明中,从服务器向重写装置发送与ECU相关的秘密信息,能够确保与ECU相关的秘密信息的机密性。

[0009] 用于解决课题的手段

[0010] 根据本发明的第一方式,由搭载在车辆上的车载通信装置、电子控制装置以及没有装载在车辆上的信息处理装置构成的车载信息通信系统,电子控制装置具备:电子控制装置存储部,其存储事先与信息处理装置共享的通用密钥;消息生成部,其生成用于认证的消息;消息认证编码生成部,其使用通用密钥生成与消息相关的消息认证编码;以及电子控制装置通信部,其将消息生成部所生成的消息以及消息认证编码生成部所生成的消息认证编码经由车载通信装置发送给信息处理装置,信息处理装置具备:信息处理装置存储部,其存储通用密钥;消息认证编码验证部,其使用通用密钥以及接收到的消息来验证接收到的消息认证编码,从而进行电子控制装置的认证;响应编码生成部,其使用通用密钥生成响应编码,其是通过对称密钥密码将基于接收到的消息的值进行加密后的响应编码;以及信息处理装置通信部,其在消息认证编码验证部的验证成功后,将响应编码生成部所生成的响应编码经由车载通信装置发送给电子控制装置,电子控制装置还具备:响应编码验证部,其根据通用密钥验证接收到的响应编码,从而进行信息处理装置的认证。

[0011] 根据本发明的第二方式,由搭载到车辆上的车载通信装置、电子控制装置以及没有装载到车辆上的信息处理装置构成的车载信息通信系统的电子控制装置和信息处理装置的认证方法为,电子控制装置生成用于认证的消息,使用事先与信息处理装置共享的通用密钥生成与消息相关的消息认证编码,将所生成的消息以及所生成的消息认证编码经由

车载通信装置发送给信息处理装置，信息处理装置使用通用密钥以及接收到的消息来验证接收到的消息认证编码，从而认证电子控制装置，根据接收到的消息以及通用密钥生成响应编码，如果验证成功，则将所生成的响应编码经由车载通信装置发送给电子控制装置，电子控制装置根据通用密钥验证接收到的响应编码，从而认证信息处理装置。

[0012] 发明的效果

[0013] 根据本发明，能够确保与ECU相关的秘密信息的机密性。

附图说明

[0014] 图1是表示第一实施方式的车载信息通信系统1的概略结构的图。

[0015] 图2是表示发送接收表117的一例的图。

[0016] 图3是表示车载通信装置131的结构框图。

[0017] 图4是表示信息管理表158的一例的图。

[0018] 图5是表示ECU132的结构框图。

[0019] 图6是表示信息处理装置101、车载通信装置131以及ECU132所具备的密钥信息的相关的图。

[0020] 图7是表示认证处理流程的迁移图。

[0021] 图8是表示ECU的密码处理1的详细的流程图。

[0022] 图9是表示车载通信装置的密码处理2的详细的流程图。

[0023] 图10是表示信息处理装置的密码处理3的详细的流程图。

[0024] 图11是表示车载通信装置的密码处理4的详细的流程图。

[0025] 图12是表示ECU的密码处理5的详细的流程图。

[0026] 图13是表示第二实施方式的密码处理1的详细的流程图。

[0027] 图14是表示第二实施方式的密码处理2的详细的流程图。

[0028] 图15是表示第二实施方式的密码处理3的详细的流程图。

具体实施方式

[0029] (第一实施方式)

[0030] 以下，参照图1～图12说明本发明的车载信息通信系统的一个实施方式。

[0031] 图1是表示本发明第一实施方式的车载信息通信系统1的概略结构的图。如图1所示，车载信息通信系统1包括信息处理装置101以及车辆103。信息处理装置101以及车辆103经由无线通信网102能够相互通信地连接。图1中，车载信息通信系统1由1个信息处理装置101以及1台车辆103构成，但是也可以由多个信息处理装置101以及多个车辆103构成。

[0032] 车辆103由车载通信装置131以及多个ECU 132构成。车载通信装置131以及多个ECU132通过车载网络133能够相互通信地连接。仅车载通信装置131与无线通信网102连接，任何一个ECU132如果不经过车载通信装置131就不能够与信息处理装置101通信。

[0033] (信息处理装置101的结构)

[0034] 信息处理装置101例如是服务器装置。如图1所示，信息处理装置101具备输入输出接口111、存储部114、可携带型存储介质接口部119、通信部120以及处理部121。输入输出接口111、存储部114、可携带型存储介质接口部119、通信部120以及处理部121经由总线118能

够相互通信地连接。存储部114中保存常数115、密钥信息116以及发送接收表117。处理部121具备密码协议控制部123和密码处理部124。

[0035] 输入输出接口111进行在处理部121与显示器112以及键盘113之间输入输出的信号的接口处理。处理部121经由输入输出接口111将信号输出给显示器112，由此显示各种信息。处理部121能够取得从键盘113经由输入输出接口111而输出的操作信号，检测针对信息处理装置101的操作者的操作，进行与该操作内容相应的处理。

[0036] 存储部114例如由ROM、RAM、NVRAM(Non Volatile RAM，非易失性RAM)、硬盘驱动器、SSD(Solid State Drive，固态硬盘)、光学存储装置等构成。存储部114中存储常数115、密钥信息116以及发送接收表117。

[0037] 常数115是在密码处理中使用的常数等，例如是椭圆曲线密码中的基点、RSA密码中的公开密钥密码指数e等。

[0038] 密钥信息116是用于认证的多个密钥的信息。这里所说的密钥是预先决定的电子数据，例如是非常大的数。后面再描述密钥的种类、性质及其运作。密钥信息116中准备有分别与通信目的地对应的密钥，在发送接收表117中记录通信目的地与密钥的对应关系。发送接收表117中包括用于识别车载通信装置131、ECU132的识别信息、以及与个别的车载通信装置131和ECU132对应的密钥信息116的识别信息。

[0039] 图2是表示发送接收表117的一例的图。发送接收表117由如下构成，即用于识别车辆103的车辆ID、用于识别车载通信装置131的车载通信装置ID、用于识别ECU132的ECUID、用于识别制造了ECU132的ECU制造公司的ECU制造公司ID、识别ECU132的固件(firmware)的版本信息的固件版本信息、用于识别在ECU132的认证中使用的密钥信息的ECU密钥信息ID、以及用于识别在车载通信装置131的认证中所使用的密钥信息的车载通信装置秘密信息ID。

[0040] 返回图1继续说明。

[0041] 可携带型存储介质接口部119是用于将可携带型的存储介质与信息处理装置101连接的接口装置。处理部121在与经由可携带型存储介质接口部119而连接的USB存储器、各种存储卡之间，进行数据的读出以及写出。

[0042] 通信部120经由无线通信网102与车辆103进行通信。

[0043] 无线通信网102是移动电话网或无线LAN。

[0044] (处理部121)

[0045] 处理部121由CPU、ROM以及RAM构成。CPU将保存在ROM中的程序在RAM中展开并执行。但是，处理部121可以由MPU代替CPU而构成，也可以连同CPU一起使用MPU。

[0046] 密码协议控制部123以及密码处理部124将保存在ROM中的程序所具有的功能表示为功能块。

[0047] 密码协议控制部123控制后述的认证处理。密码处理部124进行在认证处理中所使用的各种密码处理。

[0048] (车载通信装置131的构成)

[0049] 图3是表示车载通信装置131的结构框图。

[0050] 车载通信装置131具备处理部151、通信部154以及存储部155。

[0051] 处理部151由CPU、ROM以及RAM构成。CPU将保存在ROM中的程序扩展到RAM并执行。

但是,处理部151可以由MPU(Micro Processing Unit,微处理单元)代替CPU而构成,也可以连同CPU一起使用MPU。

[0052] 密码协议控制部152以及密码处理部153将保存在ROM中的程序所具有的功能表示为功能块。

[0053] 密码协议控制部152控制后述的认证处理。密码处理部153进行在认证处理中所使用的各种密码处理。

[0054] 通信部154经由无线通信网102与信息处理装置101进行通信,经由车载网络133与ECU132进行通信。

[0055] 存储部155例如由ROM(Read Only Memory,只读存储器)、RAM(Random Access Memory,随机存取存储器)、NVRAM(Non Volatile RAM,非易失性RAM)、硬盘驱动器、SSD、光学存储装置等构成。存储部155中存储常数156、密钥信息157以及信息管理表158。

[0056] 常数156是通过密码处理而使用的常数等,例如是椭圆曲线密码中的基点、RSA密码中的公开密钥密码指数e等。

[0057] 密钥信息157是在认证中使用的多个密钥的信息。后面再描述密钥的种类及其运作。密钥信息157中准备与各个通信目的地对应的密钥,在发送接收表158中记录通信目的地与密钥的对应关系。信息管理表158中包括用于识别信息处理装置101的识别信息、以及与个别的信息处理装置101对应的密钥信息157的识别信息。

[0058] 图4是表示信息管理表158的一例的图。

[0059] 信息管理表158用于由车载通信装置131进行与车辆103内的车载网络连接的ECU132的识别、ECU132的固件版本信息的管理。

[0060] 信息管理表158由如下构成,即用于识别车辆103的车辆ID、用于识别通信目的地的信息处理装置101的信息处理装置ID、用于识别ECU132的ECUID、用于识别制造了ECU132的ECU制造公司的ECU制造公司ID、用于识别ECU132的固件的版本信息的固件版本信息、以及用于识别在信息处理装置101的认证中所使用的密钥信息157的信息处理装置秘密信息ID。

[0061] (ECU132的结构)

[0062] 图5是表示ECU132的结构框图。

[0063] ECU132具备处理部171、通信部174以及存储部175。

[0064] 处理部171由CPU、ROM以及RAM构成。CPU将保存在ROM中的程序扩展到RAM并执行。但是,处理部171可以由MPU(Micro Processing Unit微处理单元)代替CPU而构成,也可以和CPU一起使用MPU。

[0065] 密码协议控制部172以及密码处理部173将保存在ROM中的程序所具有的功能表示为功能块。

[0066] 密码协议控制部172控制后述的认证处理。密码处理部173进行认证处理所使用的各种密码处理。如果由用户接通车辆103所具备的未图示的点火钥匙,则密码协议控制部172开始后述的处理。

[0067] 通信部174经由车载网络133与车载通信装置131进行通信。

[0068] 存储部175由例如ROM、RAM、NVRAM、硬盘驱动器、SSD、光学存储装置等构成。存储部175中存储常数176以及密钥信息177。

[0069] 常数176是在密码处理中使用的常数等，例如是椭圆曲线密码中的基点、RSA密码中的公开密钥密码指数e等。

[0070] 密钥信息177是在与特定的信息处理装置101的认证中使用的多个密钥的信息。后面再描述密钥的种类及其运作。ECU132只与特定的信息处理装置101进行通信，所以不会如信息处理装置101或车载通信装置131那样具有与多个通信目的地对应的密钥。因此，也不具有相当于发送接收表117、信息管理表158的信息。

[0071] (密钥信息)

[0072] 使用图6说明保存在信息处理装置101中的密钥信息116、保存在车载通信装置131中的密钥信息157以及保存在ECU132中的密钥信息177。但是，只表示图6中的某一组信息处理装置101、车载通信装置131以及ECU132的认证中所使用的密钥信息。图6的图示上下方向的高度相同的密钥表示存在相同或相关。

[0073] 图6是表示信息处理装置101、车载通信装置131以及ECU132所具备的密钥信息的相关的图。信息处理装置101具备通用密钥CK1、第一秘密密钥SKS、以及第二公开密钥PKT。车载通信装置131具备第一公开密钥PKS和第二秘密密钥SKT。ECU132具备密钥K、密钥密码密钥(密钥加密密钥)KEK以及通用密钥CK2。密钥K、密钥密码密钥KEK以及通用密钥CK2是ECU132所具有的秘密信息。密钥K例如是从外部向ECU132输出动作指令时所需要的信息。

[0074] ECU132所具备的密钥K以及密钥密码密钥KEK是仅ECU132所具备的密钥。

[0075] 信息处理装置101所具备的通用密钥CK1与ECU132所具备的通用密钥CK2相同，这些是所谓的共享秘密密钥。通用密钥CK1以及通用密钥CK2事先通过安全的分配单元由信息处理装置101和ECU132来共享。

[0076] 第一秘密密钥SKS和第一公开密钥PKS是与公开密钥密码对应的一对密钥、所谓的密钥对。第二公开密钥PKT和第二秘密密钥SKT也同样是与公开密钥密码对应的一对密钥、所谓的密钥对。第一秘密密钥SKS以及第二秘密密钥SKT是所谓的私钥。第一公开密钥PKS以及第二公开密钥PKT是所谓的公钥。

[0077] 在信息处理装置101与ECU132之间使用通用密钥CK1以及通用密钥CK2来相互进行认证。在信息处理装置101与车载通信装置131之间，一方使用秘密密钥生成电子署名(以下称为署名)，另一方使用相应的公开密钥来验证该署名，由此进行认证。

[0078] (认证处理的概要)

[0079] 说明信息处理装置101、车载通信装置131以及ECU132的认证处理的概要。

[0080] 图7是表示认证处理的概要的迁移图。图示中，时间从上向下地经过。

[0081] ECU132的处理部171在车辆103的点火开关被接通后，从存储部175读入密钥信息177(步骤S511)。ECU132的处理部171使用在步骤S511取得的密钥信息177来实施密码处理1(步骤S512)。步骤S512的密码处理1例如由后述的图8的流程图来实现。ECU132的通信部174将在步骤S512所生成的信息发送给被装载到相同车辆103上的车载通信装置131(步骤S513)。

[0082] 如果车载通信装置131接收到在步骤S513发送来的数据，则车载通信装置131的处理部151从存储部155读入密钥信息157(步骤S521)。

[0083] 车载通信装置131的处理部151使用在步骤S513接收到的数据以及在步骤S521取得的密钥信息157来实施密码处理2(步骤S522)。步骤S522的密码处理2例如由后述的图9的

流程图来实现。

[0084] 车载通信装置131的通信部154将在步骤S522生成的信息等经由无线通信网102发送给信息处理装置101(步骤S523)。

[0085] 如果信息处理装置101接收到在步骤S523发送来的数据,则信息处理装置101的处理部121读入存储在存储部114中的密钥信息116(步骤S531)。

[0086] 信息处理装置101的处理部121使用接收到的数据以及在步骤S531取得的密钥信息116来实施密码处理3(步骤S532)。步骤S532的密码处理3例如通过后述的图10的流程图来实现。在该密码处理3中,进行基于信息处理装置101的车载通信装置131以及ECU132的认证。

[0087] 信息处理装置101的通信部120将在步骤S532生成的数据发送给车载通信装置131(步骤S533)。

[0088] 如果车载通信装置131接收到在步骤S533发送来的数据,则车载通信装置131的处理部151从存储部155读入密钥信息157(步骤S541)。处理部151使用在步骤S541取得的密钥信息157以及接收到的数据来实施密码处理4(步骤S542)。步骤S542的密码处理4例如由后述的图11的流程图来实现。在该密码处理4中,进行基于车载通信装置131的信息处理装置101的认证。

[0089] 车载通信装置131的通信部154将包括在步骤S542生成的信息的数据发送给ECU132(步骤S543)。

[0090] 如果ECU132接收到在步骤S543发送来的数据,则ECU132的处理部171从存储部175读入密钥信息177(步骤S551)。

[0091] ECU132的处理部171使用在步骤S551取得的信息来实施密码处理5(步骤S552)。步骤S552的密码处理5例如由后述的图12的流程图来实现。在该密码处理5中,进行基于ECU132的信息处理装置101以及车载通信装置131的认证。

[0092] ECU132的通信部174将步骤S552的认证结果发送给车载通信装置131(步骤S561)。

[0093] 如果车载通信装置131接收到在步骤S561发送来的判定结果,则车载通信装置131的处理部151将判定结果存储在存储部155中。通信部154将接收到的判定结果发送给信息处理装置101(步骤S562)。

[0094] 如果信息处理装置101接收到在步骤S562发送来的判定结果,则信息处理装置101的处理部121将判定结果存储在存储部114中。

[0095] ECU132的处理部171在步骤S561的执行结束时,读出存储在存储部175中的认证的判定结果,判断认证是否成功。当判断为认证成功时进入步骤S572,当判断为认证失败时,结束(步骤S571)。ECU132的处理部171在步骤S571判断为认证成功时,转到固件写入时序(步骤S572)。

[0096] 车载通信装置131的处理部151在步骤S562的执行结束后,读出存储在存储部155中的认证的判定结果,判断认证是否成功。当判断为认证成功时,进入步骤S582,当判断为认证失败时,结束(步骤S581)。车载通信装置131的处理部151在步骤S581判断为认证成功时,转到固件写入时序(步骤S582)。

[0097] 信息处理装置101的处理部121将步骤S562的接收作为触发,判断认证是否成功。当判断为认证成功时,进入步骤S592,当判断认证失败时,结束(步骤S591)。

[0098] 信息处理装置101的处理部121在步骤S591中判断为认证成功时，转到固件写入时序(步骤S592)。

[0099] 在步骤S572、步骤S582以及步骤S592的固件写入时序中，信息处理装置101、车载通信装置131、ECU132相互进行通信的同时，进行固件更新处理。在该固件更新处理中，可以重新实施固件的加密解密处理、署名的生成、消息认证编码(Message Authentication Code，以下有时也标记为“MAC”)的生成、署名或MAC的验证等的安全功能，不管其方法。

[0100] (密码处理的详细)

[0101] 以下，使用图8～图12详细说明图7中表示的密码处理1～5。

[0102] (密码处理1的流程图)

[0103] 图8是表示图7中作为步骤S512所表示的密码处理1的具体例的流程图。以下所说明的各个步骤的执行主体是ECU132的密码协议控制部172。密码协议控制部172在车辆103的点火开关被设为接通时，开始以下的处理。

[0104] 在步骤S601中，密码协议控制部172使密码处理部173生成随机数r0，存储在存储部175中。接着进入步骤S602。

[0105] 在步骤S602中，密码协议控制部172使密码处理部173使用密钥密码密钥KEK将密钥K进行密码。在本步骤中所使用的密钥K以及密钥密码密钥KEK是作为密钥信息177保存在存储部175中的信息。以下将在本步骤中通过密码处理部173生成的数据称为加密数据X。这里，如果用“密码文＝$ENC_{加密密钥}$(纯文本)”的格式表示密码文的生成，则通过以下的公式1表示本步骤的处理。

[0106] $X=Enc_{KEK}(K)$……(公式1)

[0107] 接着进入步骤S603。

[0108] 在步骤S603中，密码协议控制部172使密码处理部173计算在步骤S602生成的加密数据X与在步骤S601生成的随机数r0的异或，作为异或Y0存储在存储部175中。这里，如果使用在○中的十字标记表示异或(exclusive or，以下有时标记为“XOR”)的算符，则通过以下的公式2表示本步骤的处理。

[0109] [数式1]

[0110] $Y0=X\oplus r0$……(公式2)

[0111] 接着进入步骤S604。

[0112] 在步骤S604中，密码协议控制部172将在步骤S603生成的异或Y0作为消息，将通用密钥K2作为密钥来生成消息认证编码Z。这里，如果用“消息认证编码＝$MAC_{密钥}$(消息)”的格式表示消息认证编码的生成，则通过以下的公式3表示本步骤的处理。

[0113] $Z=MAC_{CK2}(Y0)$……(公式3)

[0114] 接着进入步骤S605。

[0115] 在步骤S605中，密码协议控制部172使用通信部174将在步骤S603生成的异或Y0以及在步骤S604生成的消息认证编码Z发送给车载通信装置131。以上，结束图8所表示的密码处理1。

[0116] (密码处理2的流程图)

[0117] 图9是表示图7中作为步骤S522表示的密码处理2的具体例的流程图。以下所说明的各个步骤的执行主体是车载通信装置131的密码协议控制部152。密码协议控制部152如

果从ECU132接收到异或Y0以及消息认证编码Z,则开始以下的处理。

[0118] 在步骤S701中,密码协议控制部152使密码处理部153执行以下的处理。即,使用被保存为密钥信息157的第二秘密密钥SKT来生成接收到的异或Y0的署名即署名σ0。接着,进入步骤S702。

[0119] 在步骤S702中,密码协议控制部152使用通信部154将在步骤S701中生成的署名σ0、接收到的异或Y0、接收到的消息认证编码Z发送给信息处理装置101。以上,结束图9所表示的密码处理2。

[0120] (密码处理3的流程图)

[0121] 图10是表示图7中作为步骤S532表示的密码处理3的具体例的流程图。以下所说明的各个步骤的执行主体是信息处理装置101的密码协议控制部123。密码协议控制部123如果从车载通信装置131接收到署名σ0、异或Y0以及消息认证编码Z,则开始以下的处理。

[0122] 在步骤S801,密码协议控制部123使密码处理部124执行以下的处理。即,使用被保存为密钥信息116的通用密钥CK1和接收到的异或Y0来验证接收到的消息认证编码Z。具体地说,与上述步骤S604同样地生成消息认证编码。接着进入步骤S802。

[0123] 在步骤S802中,密码协议控制部123判断接收到的消息认证编码Z是否正当。换言之,判断接收到的消息认证编码Z与在步骤S801所生成的消息认证编码是否一致。当判断为接收到的消息认证编码Z正当、即接收到的消息认证编码Z与在步骤S801中所生成的消息认证编码一致时,进入步骤S803。当判断为接收到的消息认证编码Z不正当、即接收到的消息认证编码Z与在步骤S801中所生成的消息认证编码不一致时,进入步骤S810。

[0124] 通过验证消息认证编码Z,来确认生成了消息认证编码Z的ECU132具有与信息处理装置101相同的通用密钥。即,通过具有相同的通用密钥,当信息处理装置101认证了生成消息认证编码Z的ECU132时,处理进入步骤S803。

[0125] 在步骤S803中,密码协议控制部123使密码处理部124执行以下的处理。即,使用被保存为密钥信息116的第二公开密钥PKT和接收到的异或Y0来验证接收到的署名σ0。

[0126] 在步骤S804中,密码协议控制部123判断接收到的署名σ0是否正当。当判断为接收到的署名σ0是正当时,进入步骤S805,当判断为接收到的署名σ0不正当时,进入步骤S810。

[0127] 通过署名σ0的验证,来确认生成了署名σ0的车载通信装置131具有与第二公开密钥PKT对应的第二秘密密钥SKT。即信息处理装置101以具有第二秘密密钥SKT作为理由来认证生成了署名σ0的车载通信装置131,处理进入步骤S805。

[0128] 在步骤S805中,密码协议控制部123使密码处理部124生成随机数r1,存储在存储部114中。接着进入步骤S806。

[0129] 在步骤S806中,密码协议控制部123使密码处理部124执行以下的处理。即,使用被保存为密钥信息116的第二公开密钥PKT对随机数r1进行加密,生成加密数据c1。通过以下的公式4表示本步骤的处理。

[0130] $c1 = Enc_{PKT}(r1)$ ……(公式4)

[0131] 接着进入步骤S807。

[0132] 在步骤S807,密码协议控制部123使密码处理部124执行以下的处理。即,计算接收到的异或Y0与随机数r1的异或,进一步使用通用密钥CK1进行加密,生成加密数据c2。通过以下的公式5表示本步骤的处理。

[0133] [数式2]

[0134] $c2 = Enc_{CK1}(Y0 \oplus r1)$ ……(公式5)

[0135] 接着进入步骤S808。

[0136] 在步骤S808，密码协议控制部123使密码处理部124执行以下的处理。即，使用被保存为密钥信息157的第一秘密密钥SKS来生成在步骤S808所生成的c2的署名即署名σ1。接着进入步骤S809。

[0137] 在步骤S809，密码协议控制部123使用通信部120将在步骤S806生成的加密数据c1、在步骤S807生成的加密数据c2以及在步骤S808生成的署名σ1发送给车载通信装置131。以上，结束通过图10表示的密码处理3。

[0138] 在步骤S802或步骤S804中判断为否定时要执行的步骤S810中，密码协议控制部123使用通信部120将验证失败的意旨发送给车载通信装置131。以上，结束通过图10表示的密码处理3。

[0139] (密码处理4的流程图)

[0140] 图11是表示图7中作为步骤S542表示的密码处理4的具体例的流程图。以下所说明的各个步骤的执行主体是车载通信装置131的密码协议控制部152。密码协议控制部152当从信息处理装置101接收加密数据c1、加密数据c2以及署名σ1时，开始以下的处理。

[0141] 在步骤S901，密码协议控制部152使密码处理部153执行以下的处理。即，使用被保存为密钥信息157的第一公开密钥PKS和接收到的加密数据c2来验证署名σ1。

[0142] 在步骤S902中，密码协议控制部152判断接收到的署名σ1是否正当。当判断为接收到的署名σ1正当时，进入步骤S903。当判断为接收到的署名σ1不正当时，进入步骤S905。

[0143] 通过验证署名σ1，来确认生成了署名σ1的信息处理装置101具有与第一公开密钥PKS对应的第一秘密密钥SKS。即，车载通信装置131以具有第一秘密密钥SKS作为理由来认证生成了署名σ1的信息处理装置101，处理进入步骤S903。

[0144] 在步骤S903中，密码协议控制部152使密码处理部153执行以下的处理。即，使用被保存为密钥信息157的第二秘密密钥SKT将接收到的加密数据c1进行解密，生成解密结果c3。如图10的步骤806所说明的那样，加密数据c1是使用第二公开密钥PKT将随机数r1进行了加密的数据。因此，如果信息处理装置101以及车载通信装置131使用正确的密钥，则解密结果c3成为随机数r1。接着进入步骤S904。

[0145] 在步骤S904中，密码协议控制部152使用通信部154将在步骤S903生成的解密结果c3以及接收到的加密数据c2发送给ECU132。以上，结束通过图11表示的密码处理4。

[0146] 在步骤S902被否定判断时所执行的步骤S905中，密码协议控制部152使用通信部154将验证失败的意旨发送给ECU132。以上，结束通过图11表示的密码处理4。

[0147] (密码处理5的流程图)

[0148] 图12是表示图7中作为步骤S552表示的密码处理5的具体例的流程图。以下所说明的各个步骤的执行主体是ECU132的密码协议控制部172。密码协议控制部172如果从车载通信装置131接收到解密结果c3以及加密数据c2，则开始以下的处理。

[0149] 在步骤S1001，密码协议控制部172使密码处理部173执行以下的处理。即，使用被保存为密钥信息177的通用密钥CK2将接收到的加密数据c2进行解密，生成解密结果d1。如果用“纯文本＝$Dec_{解密密钥}$(密码文)”的格式表示纯文本的生成，则通过以下的公式6表示本步

骤的处理。

[0150] $d1=Dec_{CK2}(c2)$……(公式6)

[0151] 接着进入步骤S1002。

[0152] 在步骤S1002中，密码协议控制部172使密码处理部173执行以下的处理。即，计算在步骤S1001生成的解密结果d1与接收到的解密结果c3的XOR即异或Y1。通过以下的公式7表示本步骤的处理。

[0153] [数式3]

[0154] $Y1=d1\oplus c3$……(公式7)

[0155] 接着进入步骤S1003。

[0156] 在步骤S1003中，密码协议控制部172使密码处理部173执行以下的处理。即，计算在步骤S1002计算出的异或Y1与在图8的步骤S601所生成的随机数r0的XOR即异或Y2。通过以下的公式8表示本步骤的处理。

[0157] [数式4]

[0158] $Y2=Y1\oplus r0$……(公式8)

[0159] 接着进入步骤S1004。

[0160] 在步骤S1004，密码协议控制部172使密码处理部173执行以下的处理。即，使用被保存为密钥信息177的密钥密码密钥KEK将在步骤S1003中计算出的异或Y2进行解密，生成解密结果d2。这里，如果用“纯文本＝$Dec_{解密密钥}$(密码文)”的格式表示纯文本的生成，则通过以下的公式9表示本步骤的处理。

[0161] $d2=Dec_{KEK}(Y2)$……(公式9)

[0162] 这里，如果将公式2以及公式5～8代入公式9，则得到公式10。

[0163] [数式5]

[0164] $d2=Dec_{KEK}((Dec_{CK2}(Enc_{CK1}((X\oplus r0)\oplus r1))\oplus c3)\oplus r0)$

[0165] ……(公式10)

[0166] 进一步，如步骤S903所述，如果信息处理装置101以及车载通信装置131使用正确的密钥，则解密结果c3成为随机数r1。进一步，如果信息处理装置101和ECU132使用正确的密钥，则通用密钥CK1与通用密钥CK2相同，所以加密与解密抵消。因此，公式10会如以下公式11那样进行变形。

[0167] [数式6]

[0168] $d2=Dec_{KEK}(X\oplus r0\oplus r1\oplus r1\oplus r0)$……(公式11)

[0169] XOR运算如果重复2次则返回原来，所以基于r0以及r1的XOR运算抵消。进一步，如果将公式1代入公式11并展开消息认证编码Z，则得到以下的公式12。

[0170] $d2=Dec_{KEK}(Enc_{KEK}(K))=K$……(公式12)

[0171] 即，可知，当在这之前所说明的所有步骤中信息处理装置101、车载通信装置131以及ECU132使用了正确的密钥时，能够得到密钥K作为d2。

[0172] 接着进入步骤S1005。

[0173] 在步骤S1005中，密码协议控制部172判断在步骤S1004计算出的解密结果d2是否与被保存为密钥信息177的密钥K一致。当判断为一致时，进入步骤S1006，当判断为不一致时进入步骤S1007。

[0174] 在步骤S1006中，密码协议控制部172判断为信息处理装置101以及车载通信装置131都是正当的通信对象，并结束通过图12表示的密码处理5。

[0175] 在步骤S1005被否定判断时所执行的步骤S1007中，密码协议控制部172判断为信息处理装置101以及车载通信装置131中的至少一方是不正当的通信对象，并结束通过图12表示的密码处理5。

[0176] 车载通信装置131如果从信息处理装置101接收到验证失败的意旨，则将验证失败的意旨发送给ECU132。即，进行与图11的步骤S905同样的处理。

[0177] ECU132如果从车载通信装置131接收到验证失败的意旨，则判断为信息处理装置101以及车载通信装置131中的至少一方是不正当的通信对象。即，进行与图12的步骤S1007相同的处理。

[0178] 根据上述的第一实施方式，得到以下的作用效果。

[0179] (1)本实施方式的车载信息通信系统1由装载到车辆103上的车载通信装置131、电子控制装置即ECU132以及没有装载到车辆上的信息处理装置101构成。电子控制装置即ECU132具备：存储部175，其存储与信息处理装置101事先共享的通用密钥CK2；消息生成部即密码处理部173，其生成用于认证的消息即异或Y0(图8的步骤S603)；MAC生成部即密码处理部173，其使用通用密钥CK2生成消息即异或Y0所相关的消息认证编码Z(图8的步骤S604)；以及通信部174，其将消息生成部生成的消息以及MAC生成部生成的消息认证编码Z经由车载通信装置131发送给信息处理装置101。信息处理装置101具备：存储部114，其存储通用密钥CK1；MAC验证部即密码处理部124，其使用通用密钥CK1以及接收到的消息来验证接收到的MAC即异或Y0，从而进行ECU132的认证(图10的步骤S801)；响应编码生成部即密码处理部124，其根据接收到的消息即异或Y0以及通用密钥CK1来生成响应编码即加密数据c2(图10的步骤S807)；以及通信部120，其在MAC验证部的验证成功时(图10的步骤S804，“是”的情况)，将响应编码生成部所生成的响应编码即加密数据c2经由车载通信装置131发送给电子控制装置即ECU132。电子控制装置即ECU132还具备：响应编码验证部即密码处理部173，其根据通用密钥CK2来验证接收到的响应编码即加密数据c2，从而进行信息处理装置101的认证(图12的步骤S1001～S1004)。

[0180] 本实施方式的认证方法是由装载到车辆103上的车载通信装置131、电子控制装置即ECU132以及没有装载到车辆上的信息处理装置101构成的车载信息通信系统中的电子控制装置即ECU132与信息处理装置101的认证方法。电子控制装置即ECU132生成用于认证的消息即异或Y0，使用事先与信息处理装置101共享的通用密钥CK2来生成消息即异或Y0所相关的消息认证编码Z，将生成的消息以及生成的消息认证编码Z经由车载通信装置131发送给信息处理装置101。信息处理装置101使用通用密钥CK1以及接收到的消息即异或Y0来验证接收到的消息认证编码Z，并根据接收到的消息以及通用密钥CK1来生成响应编码即加密数据c2，如果验证成功，则将所生成的响应编码经由车载通信装置131发送给电子控制装置132。电子控制装置即ECU132根据通用密钥CK2来验证接收到的响应编码。

[0181] 根据上述的车载信息通信系统1的结构以及认证方法，对转播信息处理装置101与ECU132的通信的车载通信装置131不发送作为秘密信息的通用密钥CK1，所以能够确保与ECU相关的秘密信息的机密性。并且，能够在确保秘密信息的机密性的同时，能够相互认证信息处理装置101和ECU132。

[0182] 信息处理装置101使用消息认证编码来认证ECU132。如以下那样进行该认证。

[0183] 信息处理装置101与ECU132事先共享通用密钥作为通用密钥CK1以及通用密钥CK2。ECU132生成异或Y0，使用通用密钥CK2生成关于异或Y0的消息认证编码Z，将异或Y0和消息认证编码Z发送给信息处理装置101。信息处理装置101使用通用密钥CK1生成关于接收到的异或Y0的消息认证编码。信息处理装置101在从ECU132接收到的消息认证编码Z与自己生成的消息认证编码一致时，承认ECU132。这是因为只有具有事先共享的通用密钥，才能够生成相同的消息认证编码。

[0184] ECU132使用对称密钥密码来认证信息处理装置101。如以下那样进行该认证。

[0185] 信息处理装置101与ECU132事先共享通用密钥作为通用密钥CK1以及通用密钥CK2。信息处理装置101使用通用密钥CK1通过对称密钥密码将基于接收到的异或Y0的值进行加密，生成加密数据c2。ECU132将接收到的加密数据c2进行解密，当解密后的值与基于异或Y0的值一致时，承认信息处理装置101。因为使用对称密钥密码，所以如果没有相同的通用密钥，则不能够生成正当的加密数据。

[0186] ECU132进行该认证所需要的计算处理主要是消息认证编码的生成和对称密钥密码的处理。即，计算负荷均小，因此即使资源贫乏的ECU132也能够充分地执行。

[0187] 在消息认证编码的生成中所使用的算法以及对称密钥密码的算法，主要在信息处理装置101和ECU132是通用的即可，不限于特定的算法。因此，能够容易地变更所使用的算法，能够增加与提高计算机功能相符合的密钥的位长，作为在算法中发现脆弱性的情况的应对，可以是变更为将来要开发的算法等。

[0188] (2)车载通信装置131具备：存储部155，其存储公开密钥密码的公开密钥即第一公开密钥PKS以及公开密钥密码的秘密密钥即第二秘密密钥SKT；第一署名生成部即密码处理部153，其使用第二秘密密钥SKT生成从电子控制装置即ECU132接收到的消息即异或Y0的电子署名即第一署名σ0(图9的步骤S701)；以及通信部154，其将从电子控制装置即ECU132接收到的消息、从电子控制装置即ECU132接收到的消息认证编码Z以及第一署名生成部所生成的第一署名发送给信息处理装置。信息处理装置101的存储部114中进一步存储与第一公开密钥PKS成对的第一秘密密钥SKS以及与第二秘密密钥SKT成对的第二公开密钥PKT。信息处理装置101具备：第一署名验证部即密码处理部124，其使用第二公开密钥PKT以及接收到的消息来验证接收到的第一署名(图10的步骤S803)；随机数生成部即密码处理部124，其生成随机数r1(图10的步骤S805)；加密部即密码处理部124，其使用第二公开密钥PKT生成将随机数生成部所生成的随机数r1进行加密的加密随机数即加密数据c1(图10的步骤S806)；以及第二署名生成部即密码处理部124，其使用第一秘密密钥SKS来生成响应编码生成部所生成的响应编码即加密数据c2的电子署名即第二署名σ1(图10的步骤S808)。响应编码生成部根据接收到的消息即异或Y0、通用CP1以及随机数r1来生成响应编码即加密数据c2。信息处理装置101的通信部120将响应编码生成部所生成的响应编码即加密数据c2、加密随机数即加密数据c1以及第二署名σ1发送给车载通信装置131。车载通信装置131还具备：第二署名验证部即密码处理部153，其使用第一公开密钥PKS以及从信息处理装置101接收到的响应编码即加密数据c2来验证接收到的第二署名σ1(图11的步骤S901)；以及解密部即密码处理部153，其使用第二秘密密钥SKT将接收到的加密随机数即加密数据c1解密为解密数据即解密结果c3(图11的步骤S903)。车载通信装置131的通信部154将从信息处理装置101接收

到的响应编码即加密数据c2以及解密数据即解密结果c3发送给电子控制装置132。电子控制装置即ECU132的响应编码验证部根据通用密钥CK2以及解密结果c3来验证接收到的加密数据c2。

[0189] 因此，具有密钥对的信息处理装置101以及车载通信装置131使用公开密钥来验证对方所生成的电子署名，从而能够进行认证。当电子署名的验证成功时，可知生成该电子署名的具有与验证所使用的公开密钥对应的秘密密钥。

[0190] 在信息处理装置101和ECU132之间进行认证，在信息处理装置101和车载通信装置131之间进行认证。因此，虽然在车载通信装置131和ECU132之间不直接进行认证，但是在车载通信装置131和ECU132之间也能够经由信息处理装置101间接地进行认证。

[0191] (3)电子控制装置即ECU132的消息生成部即密码处理部173在装载了该电子控制装置的车辆103的点火开关被设为接通时，生成消息即异或Y0(图8的步骤S603)。MAC生成部即密码处理部173在消息生成部生成消息时生成消息认证编码Z(图8的步骤S604)。通信部174在MAC生成部生成消息认证编码Z时，发送由消息生成部所生成的消息以及MAC生成部所生成的消息认证编码Z。

[0192] 车载通信装置131以及ECU132在车辆103处于行驶状态时处理很多的数据，难以确保计算资源。因此，当计算资源比较富裕的车辆103开始启动时，即通过操作员将点火开关设为接通时能够进行认证。

[0193] (4)电子控制装置即ECU132还具备生成第二随机数r0的第二随机数生成部即密码处理部173(图8的步骤S601)。电子控制装置即ECU132的存储部175中还存储第一秘密信息即密钥K以及第二秘密信息即密钥密码密钥KEK。消息生成部即密码处理部173使用密钥密码密钥KEK将密钥K加密并生成加密数据X，计算加密数据X与第二随机数生成部所生成的第二随机数r0之间的位运算即异或，生成消息即异或Y0。

[0194] 因此，每次执行密码处理1时生成新的随机数r0，每次生成不同的异或Y0。所生成的随机数中没有规律，因此即使无线通信网102的通信被第三者拦截，也不能够预测接下来生成的随机数以及根据随机数生成的异或Y0，所以，能够提高安全性。

[0195] (变形例1)

[0196] 在上述第一实施方式中，在图9的步骤S701的署名生成处理和图11的步骤S903的解密处理中，使用了相同的秘密密钥即都使用了第二秘密密钥SKT。但是也可以分别准备署名生成/验证用的密钥对、加密/解密用的密钥对。

[0197] 例如，信息处理装置101的密钥信息116还存储第三公开密钥PKU，车载通信装置131的密钥信息157还存储第三秘密密钥SKU，如以下那样使用密钥。车载通信装置131在图9的步骤S701中与第一实施方式同样地使用第二秘密密钥SKT，在图11的步骤S903中使用第三秘密密钥SKU。信息处理装置101在图10的步骤S803中与第一实施方式1同样地使用第二公开密钥PKT，在步骤S806中使用第三公开密钥PKU。

[0198] 根据该变形例1，能够进一步提高安全性。

[0199] (变形例2)

[0200] 在上述第一实施方式中，存储密钥K以及密钥密码密钥KEK作为ECU132的密钥信息177。但是，在密码处理部173生成随机数r0时还生成2个随机数，可以将这些代替密钥K以及密钥密码密钥KEK。进一步，将如上述那样所生成的2个随机数保存为密钥K以及密钥密码密

钥KEK而使用，如果图8的步骤S601执行固定次数则重新进一步生成2个随机数，并可以更新密钥K以及密钥密码密钥KEK。

[0201] (变形例3)

[0202] 在上述第一实施方式中，如果通过用户将点火键设为接通，则通过ECU132开始图7所示的步骤S511以及步骤S512的处理，之后的处理在前段的处理结束之后，立刻开始处理。但是，开始各个步骤处理的定时不限于此。

[0203] 例如，可以根据用户或信息处理装置101的指令开始步骤S511以及步骤S512的处理。当车载通信装置131和ECU132的处理负荷在预定阈值以下时，可以开始步骤S511以及步骤S512的处理。

[0204] 即使前段的处理结束后，也可以不开始接下来的处理而直到该设备的处理负荷成为预定阈值以下为止，也可以只在满足了预定条件时开始接下来的处理。例如，只有在信息处理装置101检测出进行通信的ECU132的固件不是最新版的情况时可以开始步骤S532的处理。

[0205] (变形例4)

[0206] 在上述第一实施方式中，ECU132的密钥信息177中存储了密钥K以及密钥密码密钥KEK两者。但是，也可以只存储密钥K以及密钥密码密钥KEK的任意一个。

[0207] 例如，当密钥信息177中没有存储密钥密码密钥KEK时，在图8的步骤S602中将密钥K作为加密数据X来使用，省略图12的步骤S1004的处理。

[0208] (变形例5)

[0209] 可以通过与上述第一实施方式不同的步骤来生成消息认证编码Z。例如，可以通过密钥密码密钥KEK将密钥K和随机数r0的异或进行加密，并使用通用密钥CK2来生成消息认证编码Z。即通过以下的公式13表示该变形例1的消息认证编码Z的计算式。

[0210] [数式7]

[0211] $Z = MAC_{CK2}(Enc_{KEK}(K \oplus r0))$ ……(公式13)

[0212] (变形例5)

[0213] 在上述第一实施方式中，在ECU132的密码处理5中，通过解密结果d2是否与密钥K一致来判断是否是正当的通信对象(图12的步骤S1005)。但是，也可以通过在步骤S1002计算出的异或Y1是否与异或Y0一致来判断是否是正当的通信对象。此时，ECU132将在图8的步骤S605中发送的异或Y0存储在存储部175中，用于上述是否一致的判断。

[0214] 根据该变形例1，能够削减资源匮乏的ECU132的计算量。

[0215] 在上述第一实施方式中，还可以进行以下的变形。

[0216] (1)信息处理装置101不一定需要具备上述所有的硬件结构，例如，可以不具备显示器112或键盘113。

[0217] (2)发送接收表117以及信息管理表158不一定必须要包括上述所有的信息，也可以包括上述信息以外的信息。例如，信息管理表158也可以包括用于识别为了认证信息处理装置101而使用的密钥信息的信息处理装置公开信息ID等。

[0218] (3)存储部114也可以存储上述信息以外的信息，例如存储车载通信装置131、ECU132的各种固件。

[0219] (4)处理部121、151、171所进行处理的一部分可以通过硬件电路来实现。例如，可

以通过随机数生成器来生成随机数。

[0220] (第二实施方式)

[0221] 参照图13～图15说明本发明的车载信息通信系统的第二实施方式。在以下说明中,对与第一实施方相同的结构要素标注相同的标记,来主要说明不同点。关于没有特别说明的点,与第一实施方式相同。在本实施方式中,主要是在固件写入时序中使用会话密钥的点与第一实施方式不同。

[0222] (结构)

[0223] 在第二实施方式的车载信息通信系统1的结构中,在信息处理装置101的存储部114以及ECU132的存储部175中保存会话密钥,这一点与第一实施方式不同。但是,会话密钥没有如密钥信息那样事先被共享,而是如后述那样开始认证流程后被生成或在被加密的状态下被运送。

[0224] 在第二实施方式中,程序的动作与第一实施方式不同。具体地说,在第一实施方式中使用图7所说明的认证处理流程的概要与第一实施方式相同,步骤S512的密码处理1、步骤S522的密码处理2以及步骤S532的密码处理3与第一实施方式不同。

[0225] (密码处理1的流程图)

[0226] 图13是表示第二实施方式的密码处理1的具体例的流程图。对与第一实施方式相同的处理赋予相同的步骤编号,省略说明。

[0227] 在步骤S604的下一个执行的步骤S1101中,密码协议控制部172使密码处理部173执行以下的处理。即,生成随机数的会话密钥SS并保存在存储部175中,使用被保存为密钥信息177的通用密钥CK2来加密会话密钥SS,生成加密会话密钥ESS。接着进入步骤S1102。

[0228] 在步骤S605中,密码协议控制部172使用通信部174将在步骤S603生成的异或Y0、在步骤S604生成的消息认证编码Z以及在步骤S1101生成的加密会话密钥ESS发送给车载通信装置131。以上,结束通过图13表示的第二实施方式的密码处理1。

[0229] (密码处理2的流程图)

[0230] 图14是表示第二实施方式的密码处理2的具体例的流程图。对与第一实施方式相同的处理赋予相同的步骤编号,省略说明。

[0231] 在步骤S701的下一个执行的步骤S1201中,密码协议控制部152使用通信部154将在步骤S701生成的署名σ0、接收到的异或Y0、接收到的消息认证编码Z以及接收到的加密会话密钥ESS发送给信息处理装置101。以上,结束通过图14表示的第二实施方式的密码处理2。

[0232] (密码处理3的流程图)

[0233] 图15是表示第二实施方式的密码处理3的具体例的流程图。对与第一实施方式相同的处理赋予相同的步骤编号,省略说明。

[0234] 在步骤S804做肯定判定而要执行的步骤S1301中,密码协议控制部123使密码处理部124执行以下的处理。即,使用被保存为密钥信息116的通用密钥CK1使接收到的加密会话密钥ESS解密,作为解密会话密钥DSS保存到存储部114中。接着进入步骤S805。

[0235] (认证结束后的通信)

[0236] ECU132在认证结束后的通信中,使用会话密钥SS将发送到信息处理装置101中的数据进行加密,使用会话密钥SS将从信息处理装置101接收到的数据进行解密。

[0237] 信息处理装置101在认证结束后的通信中，使用解密会话密钥DSS将发送到ECU132中的数据进行加密，使用解密会话密钥DSS将从ECU132接收到的数据进行解密。

[0238] 如果信息处理装置101以及ECU132使用正确的密钥，则会话密钥SS和解密会话密钥DSS相同，所以能够将信息处理装置101与ECU132之间的通信进行加密。

[0239] 根据上述第二实施方式，得到以下的作用效果。

[0240] (1)ECU132生成在认证结束后的通信中使用的会话密钥SS，并通过通用密钥CK2进行加密来生成加密会话密钥ESS，发送给信息处理装置101。信息处理装置101通过通用密钥CK1将接收到的加密会话密钥密钥ESS进行解密并得到解密会话密钥DSS。

[0241] 因此，能够使用会话密钥SS以及解密会话密钥DSS来对认证结束后的通信进行加密。另外，每次执行密码处理1时生成该会话密钥SS，所以即使有时会话密钥SS泄露到外部，影响也是有限的。

[0242] 可以分别组合上述各个实施方式以及变形例。

[0243] 上述说明了各种实施方式以及变形例，但是本发明不限于这些内容。在本发明的技术思想范围内考虑到的其他方式也包括在本发明的范围内。

[0244] 以下的作为优先权基础申请的公开内容作为引用文被合并到这里。

[0245] 日本国专利申请2015年第130315号(2015年6月29日申请)

[0246] 附图标记的说明

[0247] 1:车载信息通信系统、101:信息处理装置、102:无线通信网、103:车辆、114、155、175:存储部、116、157、177:密钥信息、117:发送接收表、120、154、174:通信部、121、151、171:处理部、123、152、172:密码协议控制部、124、153、173:密码处理部、131、154、174:车载通信装置、132:ECU、158:信息管理表、K:密钥、X:加密数据、Z:消息认证编码、SS:会话密钥、YO:异或、c1、c2:加密数据、c3:解密结果、d1、d2:解密结果、r0、r1:随机数、CK1:通用密钥、CK2:通用密钥、KEK:密钥密码密钥、PKS:第一公开密钥、PKT:第二公开密钥、SKS:第一秘密密钥、SKT:第二秘密密钥。

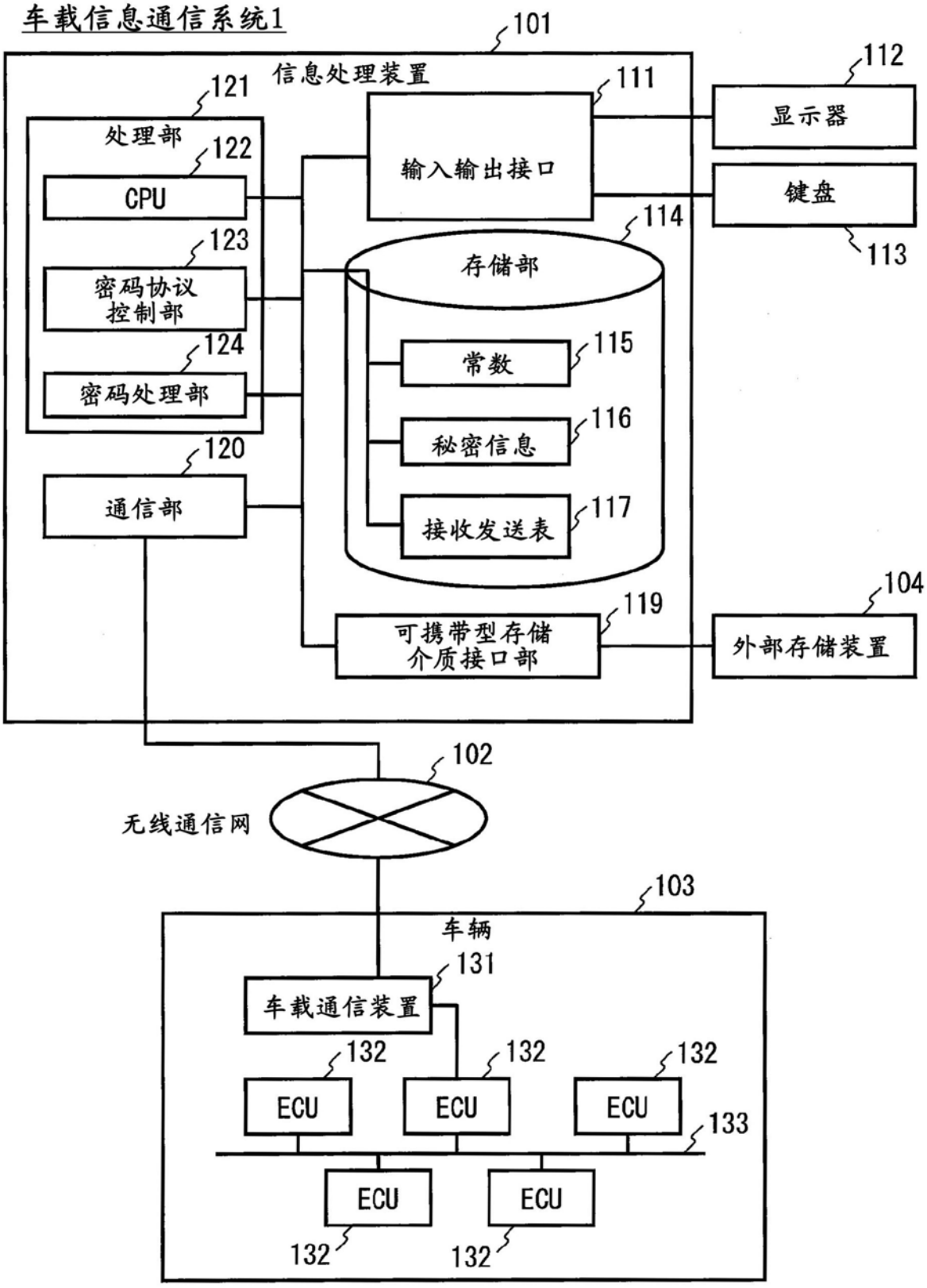

车载信息通信系统1
101
信息处理装置
121
处理部
122
CPU
123
密码协议控制部
124
密码处理部
120
通信部
111
输入输出接口
112
显示器
键盘
113
114
存储部
115
常数
116
秘密信息
117
接收发送表
119
可携带型存储介质接口部
104
外部存储装置
102
无线通信网
103
车辆
131
车载通信装置
132
ECU
133

图1

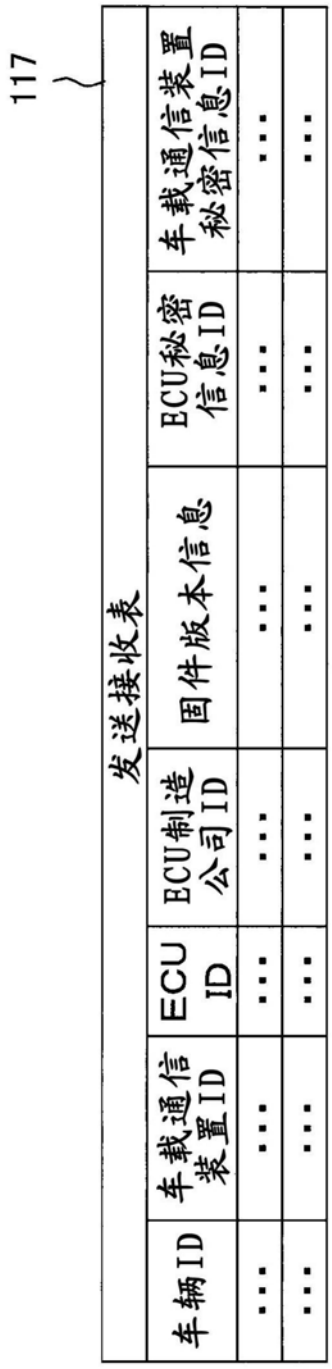

117
发送接收表
车辆ID
车载通信装置ID
ECU ID
ECU制造公司ID
固件版本信息
ECU秘密信息ID
车载通信装置秘密信息ID

图2

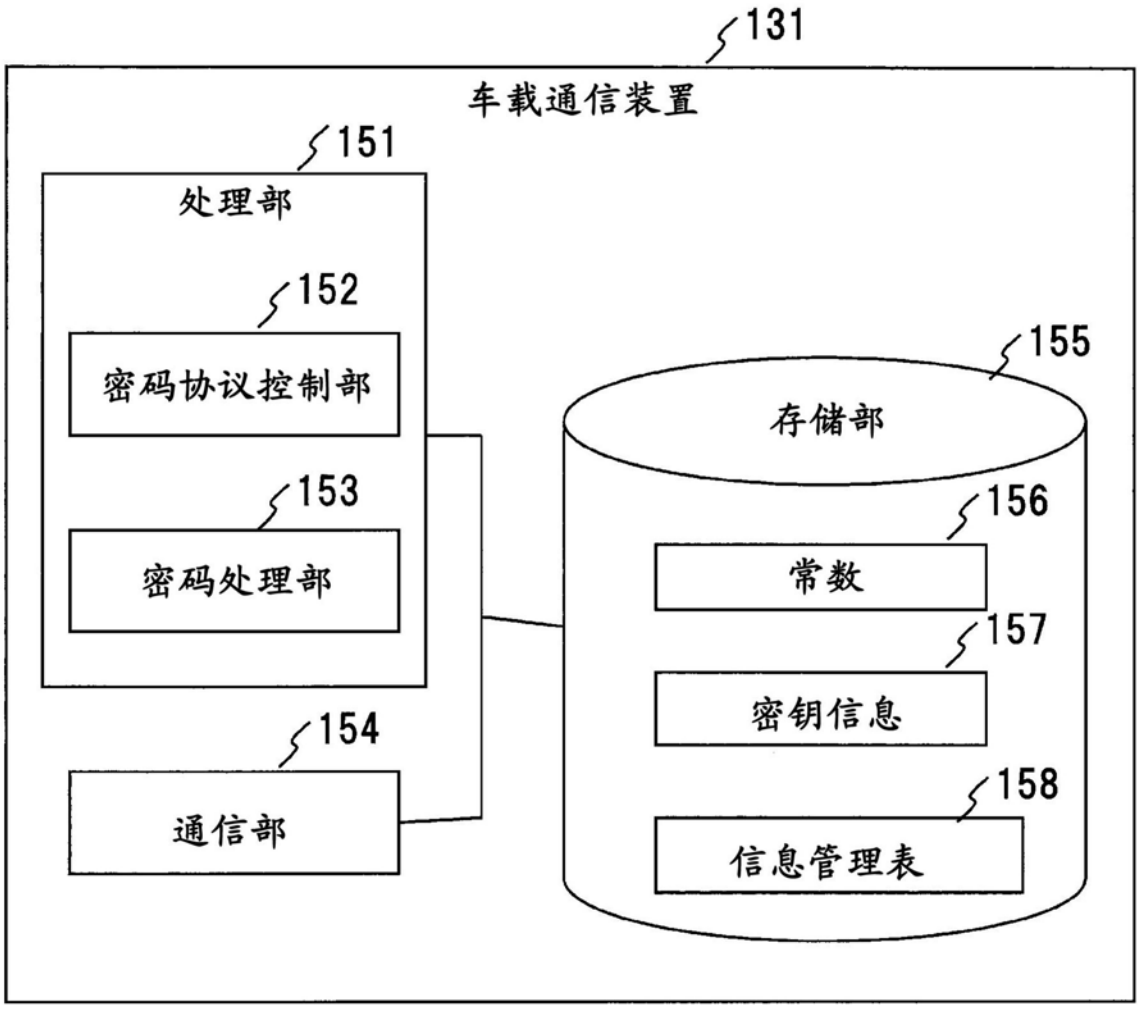

131
车载通信装置
151
处理部
152
密码协议控制部
153
密码处理部
154
通信部
155
存储部
156
常数
157
密钥信息
158
信息管理表

图3

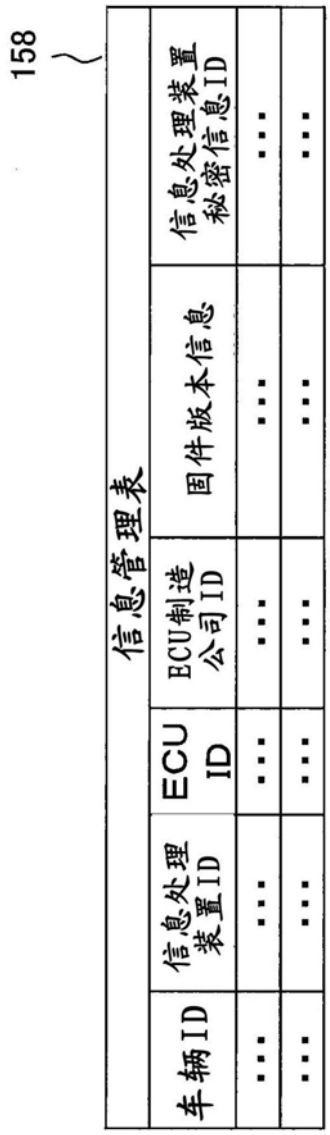

158
信息管理表
车辆ID
信息处理装置ID
ECU ID
ECU制造公司ID
固件版本信息
信息处理装置秘密信息ID
...
...
...
...
...
...
...
...
...
...
...
...

图4

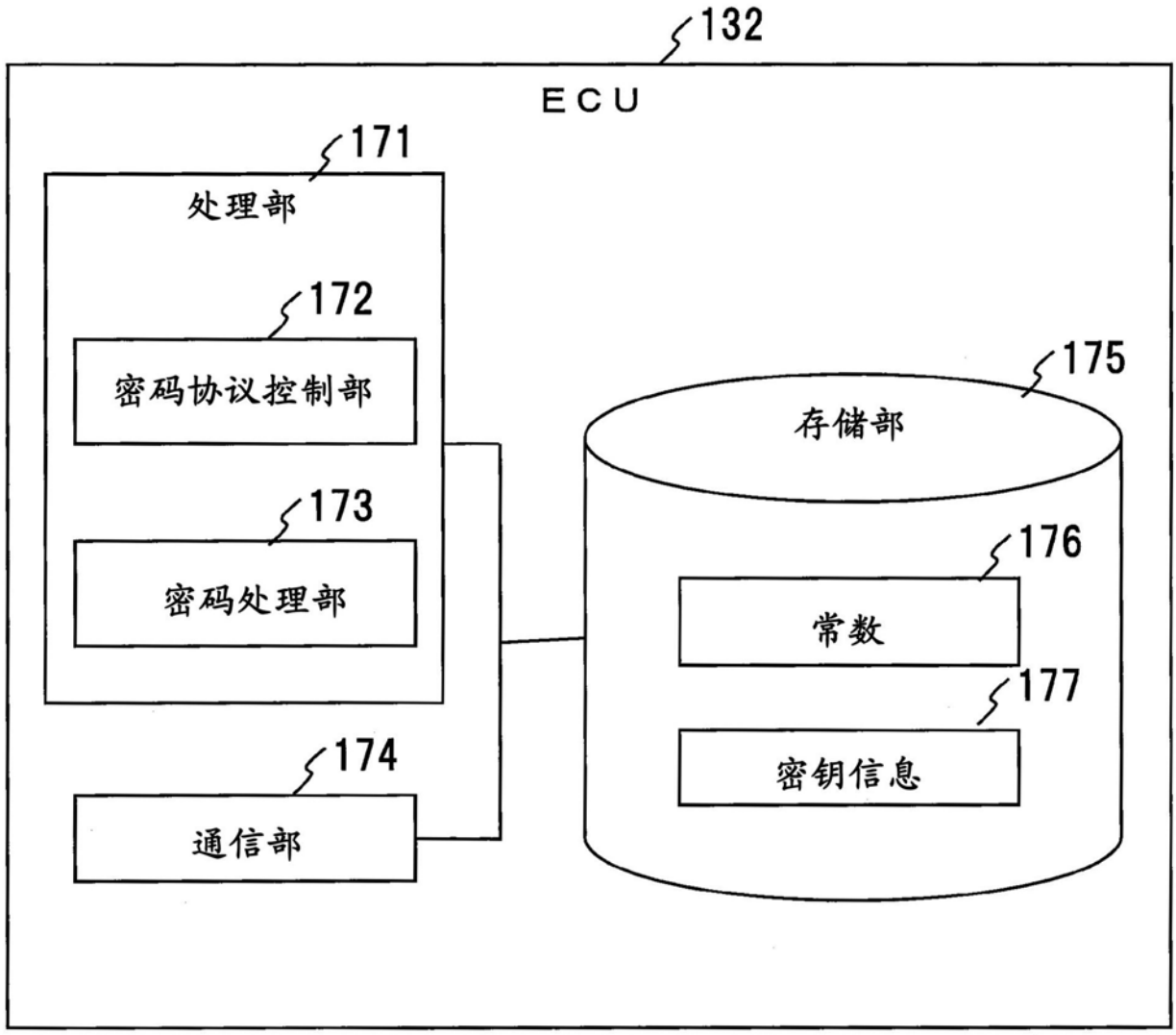

132
ECU
171
处理部
172
密码协议控制部
173
密码处理部
174
通信部
175
存储部
176
常数
177
密钥信息

图5

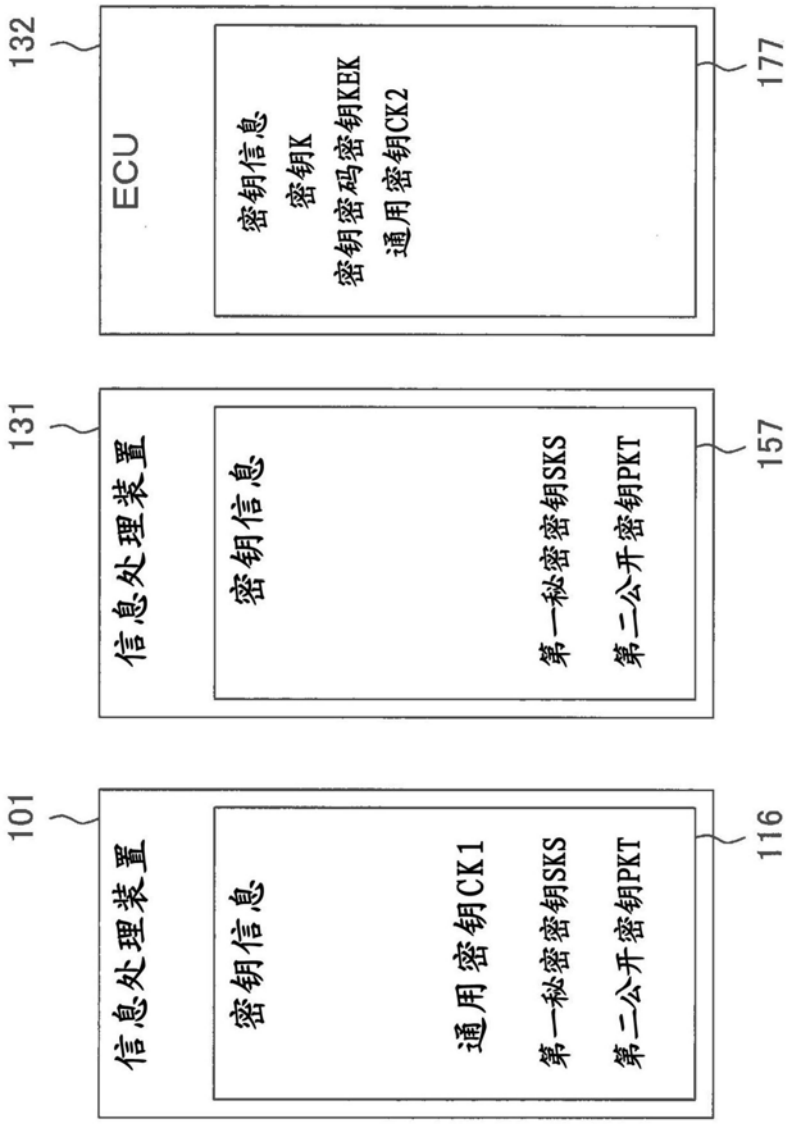

132
ECU
密钥信息
密钥K
密钥密码密钥KEK
通用密钥CK2
177
131
信息处理装置
密钥信息
第一秘密密钥SKS
第二公开密钥PKT
157
101
信息处理装置
密钥信息
通用密钥CK1
第一秘密密钥SKS
第二公开密钥PKT
116

图6

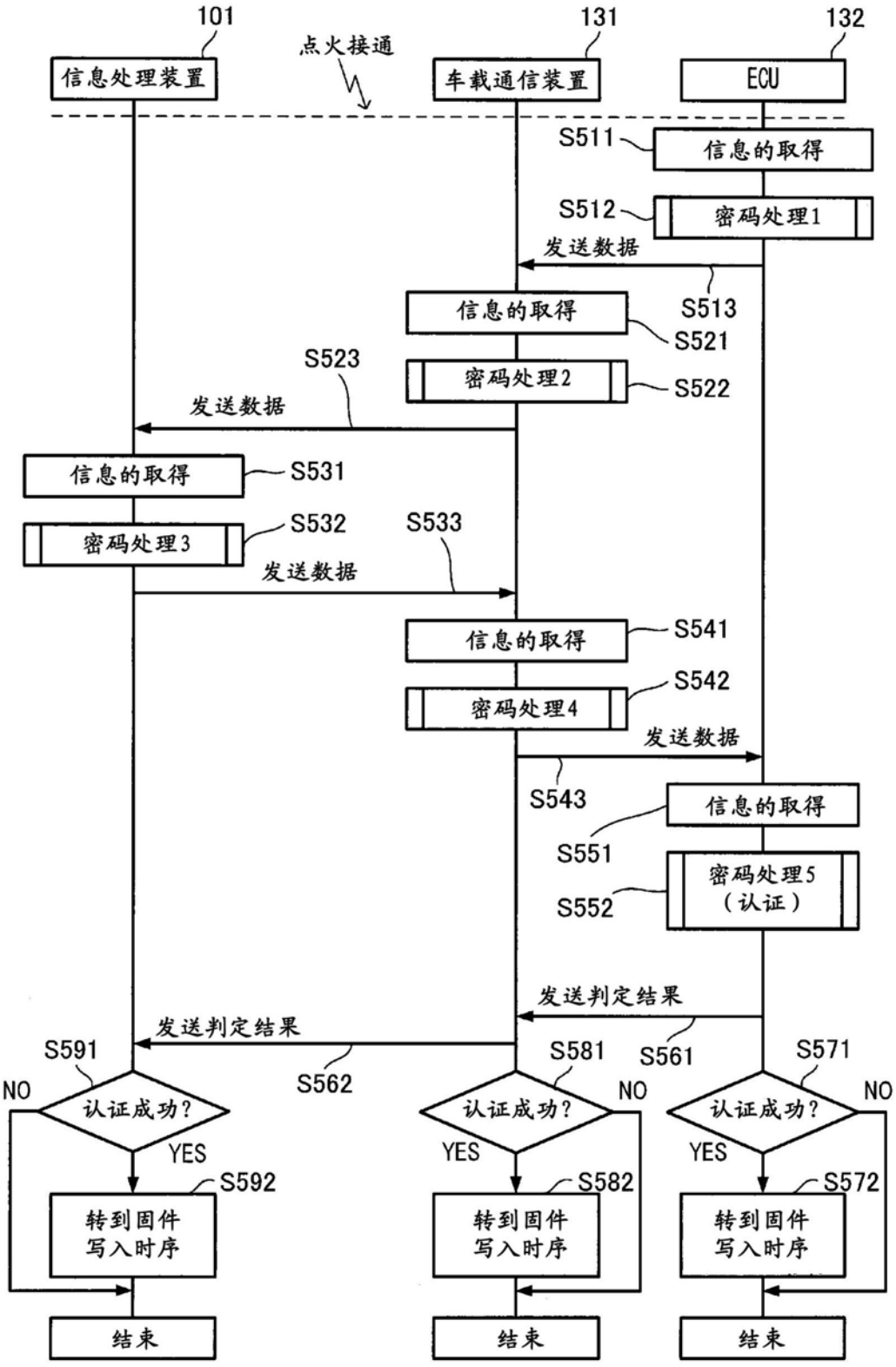

101
131
132
信息处理装置
点火接通
车载通信装置
ECU
S511
信息的取得
S512
密码处理1
发送数据
S513
信息的取得
S521
S523
密码处理2
S522
发送数据
信息的取得
S531
密码处理3
S532
S533
发送数据
信息的取得
S541
密码处理4
S542
发送数据
S543
信息的取得
S551
密码处理5
（认证）
S552
发送判定结果
发送判定结果
S591
S581
S561
S571
NO
认证成功？
NO
认证成功？
NO
认证成功？
YES
YES
YES
S592
S582
S572
转到固件
写入时序
转到固件
写入时序
转到固件
写入时序
结束
结束
结束

图7

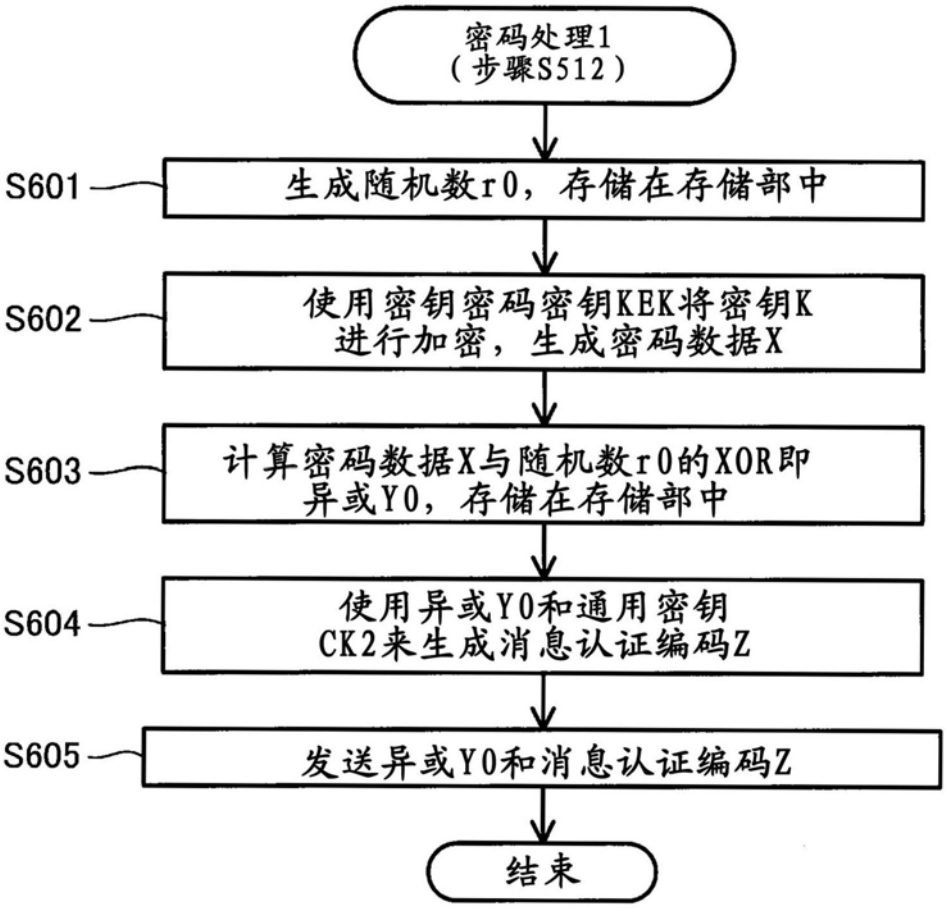

密码处理1
（步骤S512）
S601
生成随机数r0，存储在存储部中
S602
使用密钥密码密钥KEK将密钥K
进行加密，生成密码数据X
S603
计算密码数据X与随机数r0的XOR即
异或Y0，存储在存储部中
S604
使用异或Y0和通用密钥
CK2来生成消息认证编码Z
S605
发送异或Y0和消息认证编码Z
结束

图8

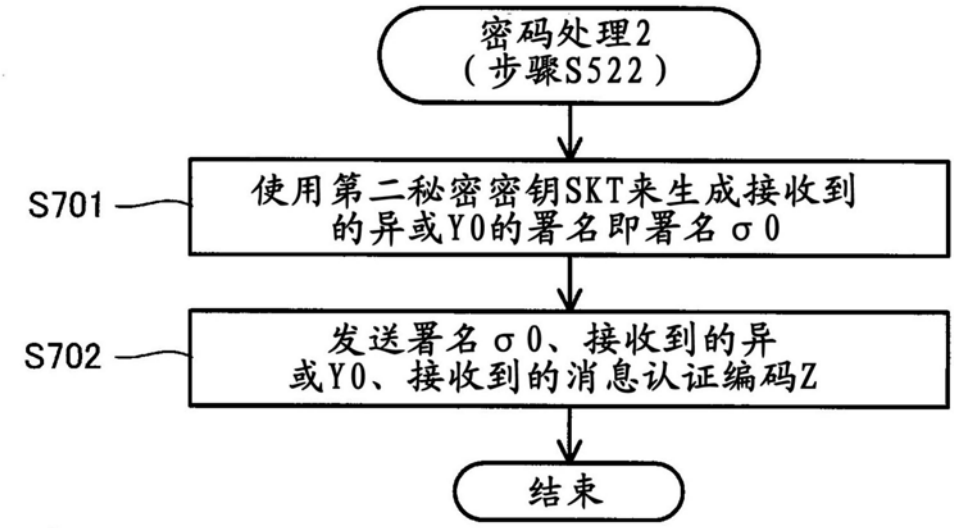

密码处理2
（步骤S522）
S701
使用第二秘密密钥SKT来生成接收到
的异或Y0的署名即署名σ0
S702
发送署名σ0、接收到的异
或Y0、接收到的消息认证编码Z
结束

图9

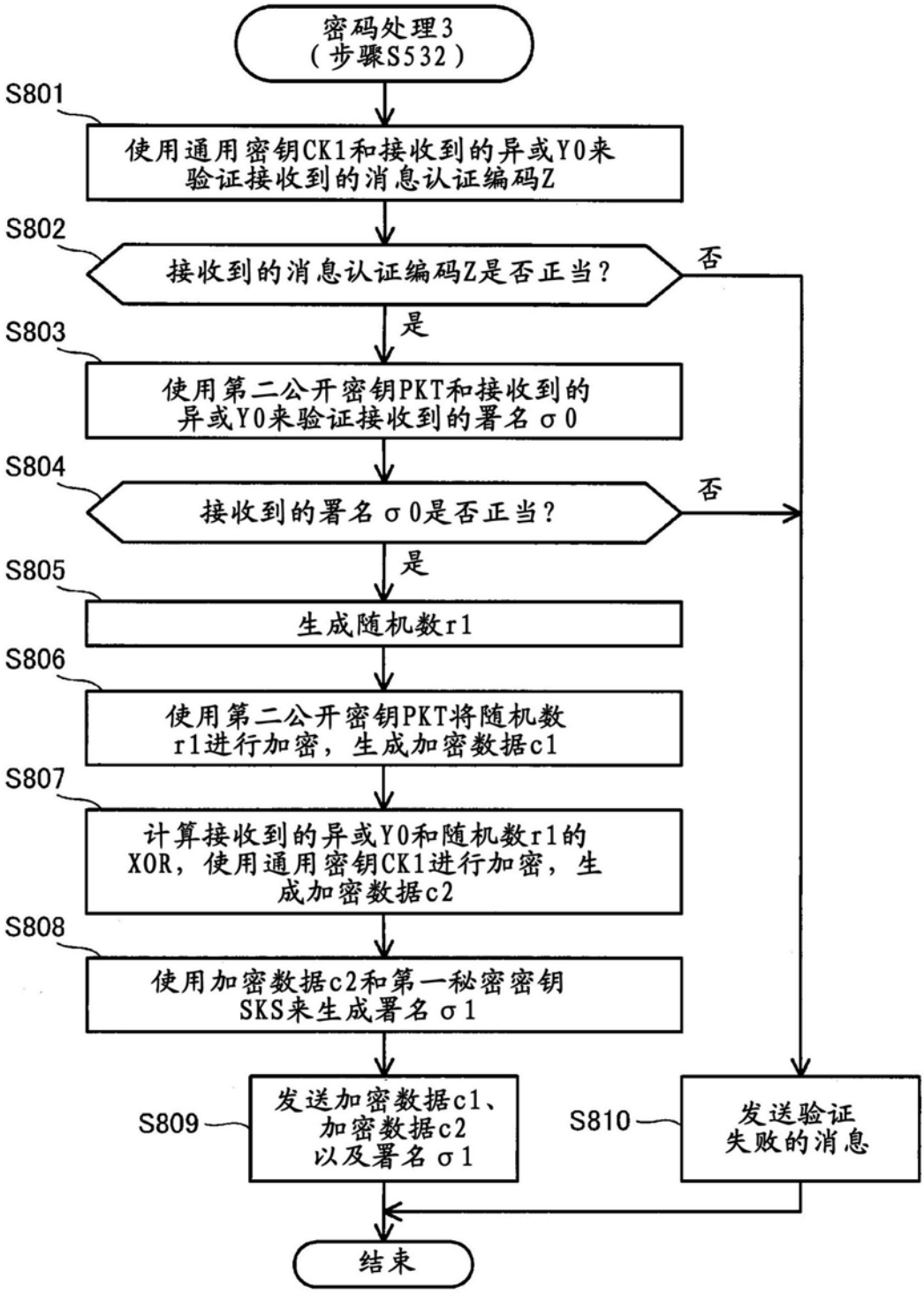

密码处理3
（步骤S532）
S801
使用通用密钥CK1和接收到的异或Y0来验证接收到的消息认证编码Z
S802
接收到的消息认证编码Z是否正当？
否
是
S803
使用第二公开密钥PKT和接收到的异或Y0来验证接收到的署名σ0
S804
接收到的署名σ0是否正当？
否
是
S805
生成随机数r1
S806
使用第二公开密钥PKT将随机数r1进行加密，生成加密数据c1
S807
计算接收到的异或Y0和随机数r1的XOR，使用通用密钥CK1进行加密，生成加密数据c2
S808
使用加密数据c2和第一秘密密钥SKS来生成署名σ1
S809
发送加密数据c1、加密数据c2以及署名σ1
S810
发送验证失败的消息
结束

图10

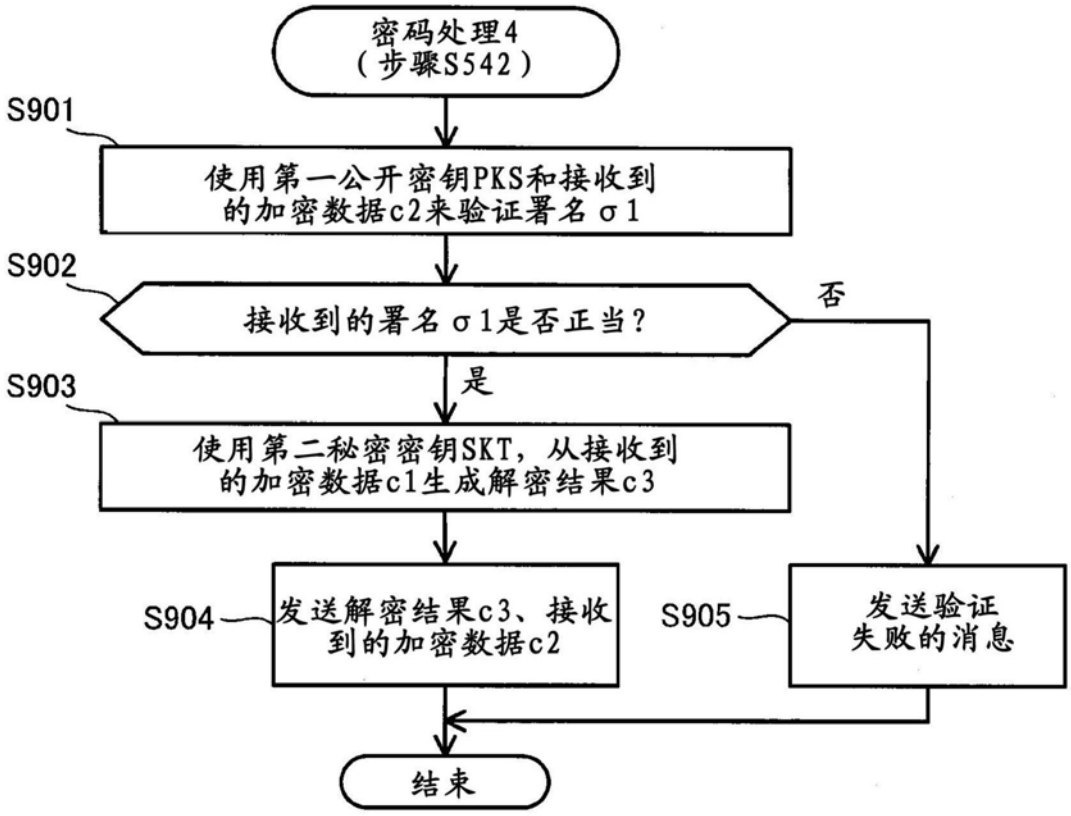

密码处理4
（步骤S542）
S901
使用第一公开密钥PKS和接收到的加密数据c2来验证署名σ1
S902
接收到的署名σ1是否正当？
否
是
S903
使用第二秘密密钥SKT，从接收到的加密数据c1生成解密结果c3
S904
发送解密结果c3、接收到的加密数据c2
S905
发送验证失败的消息
结束

图11

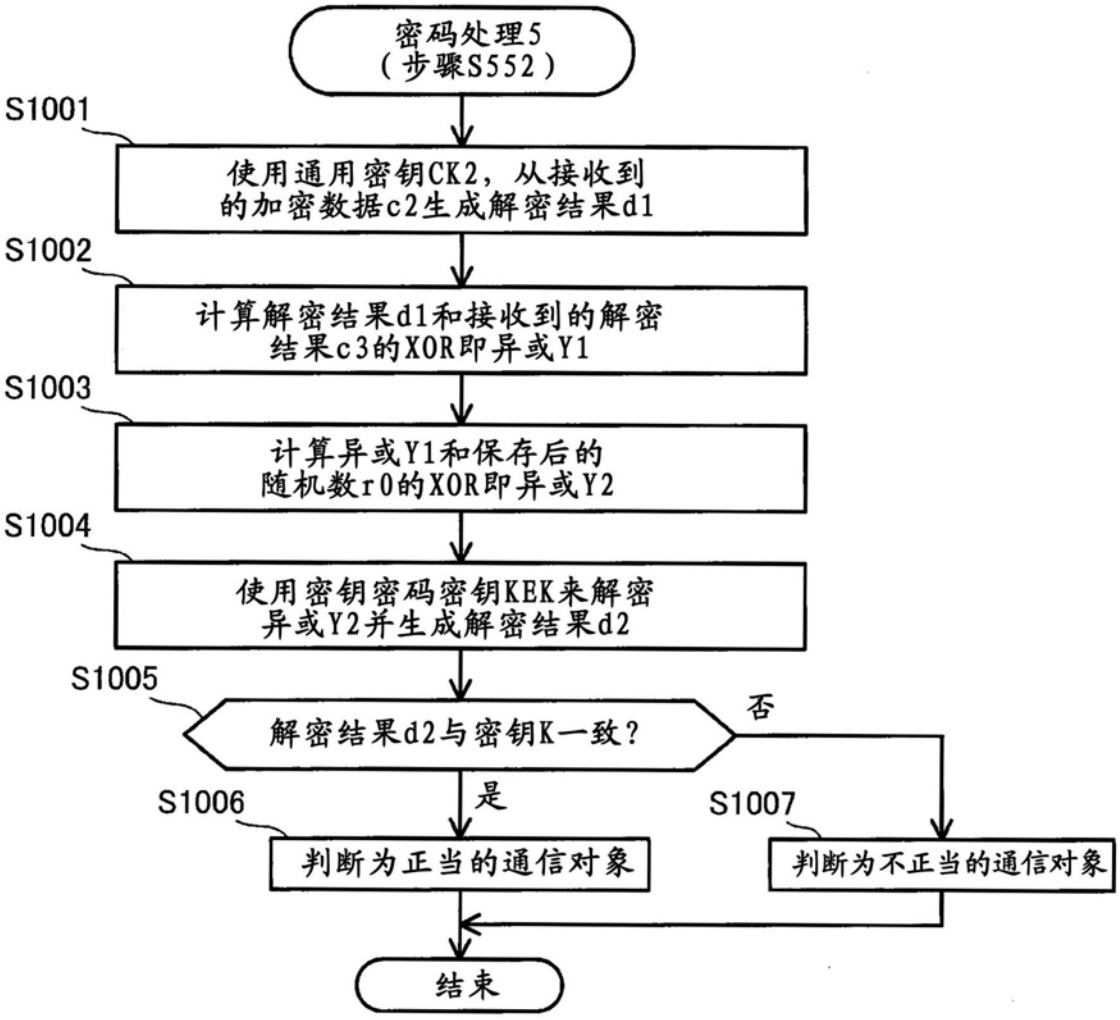

密码处理5
（步骤S552）
S1001
使用通用密钥CK2，从接收到的加密数据c2生成解密结果d1
S1002
计算解密结果d1和接收到的解密结果c3的XOR即异或Y1
S1003
计算异或Y1和保存后的随机数r0的XOR即异或Y2
S1004
使用密钥密码密钥KEK来解密异或Y2并生成解密结果d2
S1005
解密结果d2与密钥K一致？
否
是
S1006
判断为正当的通信对象
S1007
判断为不正当的通信对象
结束

图12

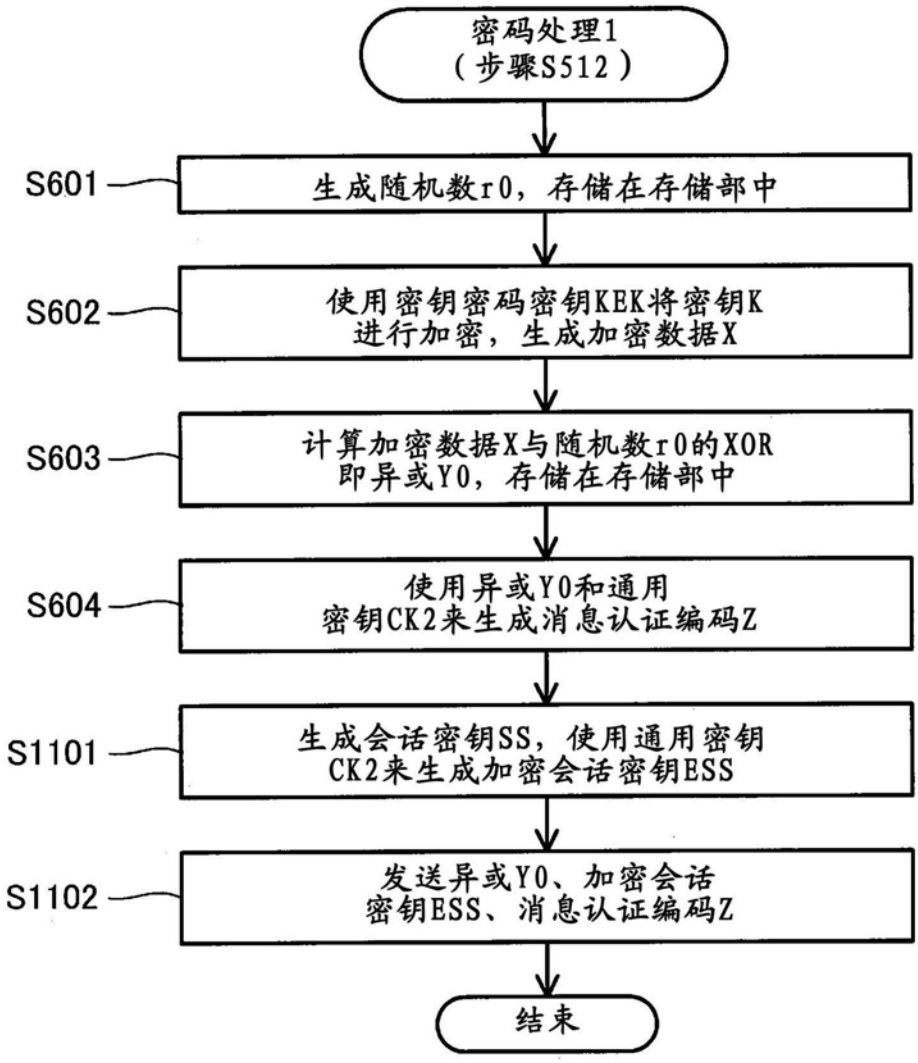

密码处理1
（步骤S512）
S601
生成随机数r0，存储在存储部中
S602
使用密钥密码密钥KEK将密钥K
进行加密，生成加密数据X
S603
计算加密数据X与随机数r0的XOR
即异或Y0，存储在存储部中
S604
使用异或Y0和通用
密钥CK2来生成消息认证编码Z
S1101
生成会话密钥SS，使用通用密钥
CK2来生成加密会话密钥ESS
S1102
发送异或Y0、加密会话
密钥ESS、消息认证编码Z
结束

图13

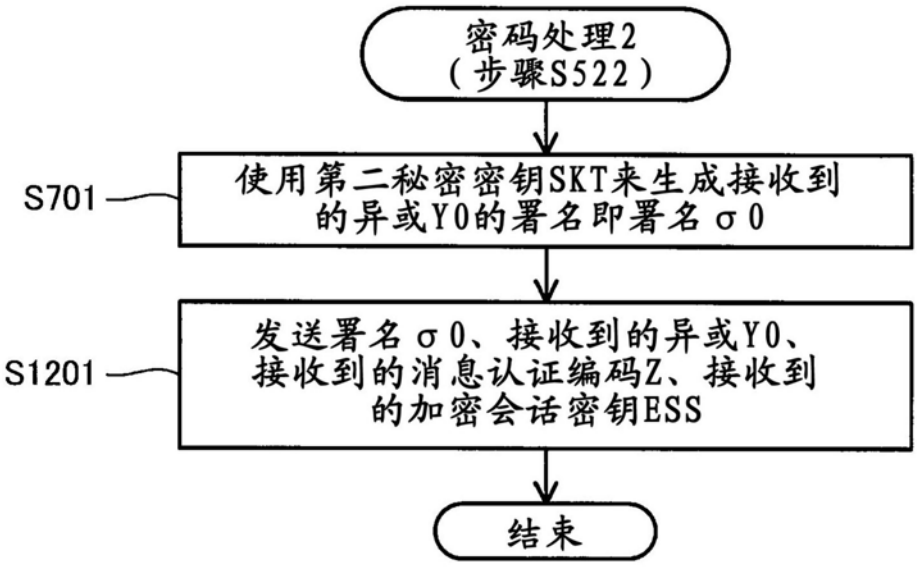

密码处理2
（步骤S522）
S701
使用第二秘密密钥SKT来生成接收到的异或Y0的署名即署名σ0
S1201
发送署名σ0、接收到的异或Y0、接收到的消息认证编码Z、接收到的加密会话密钥ESS
结束

图14

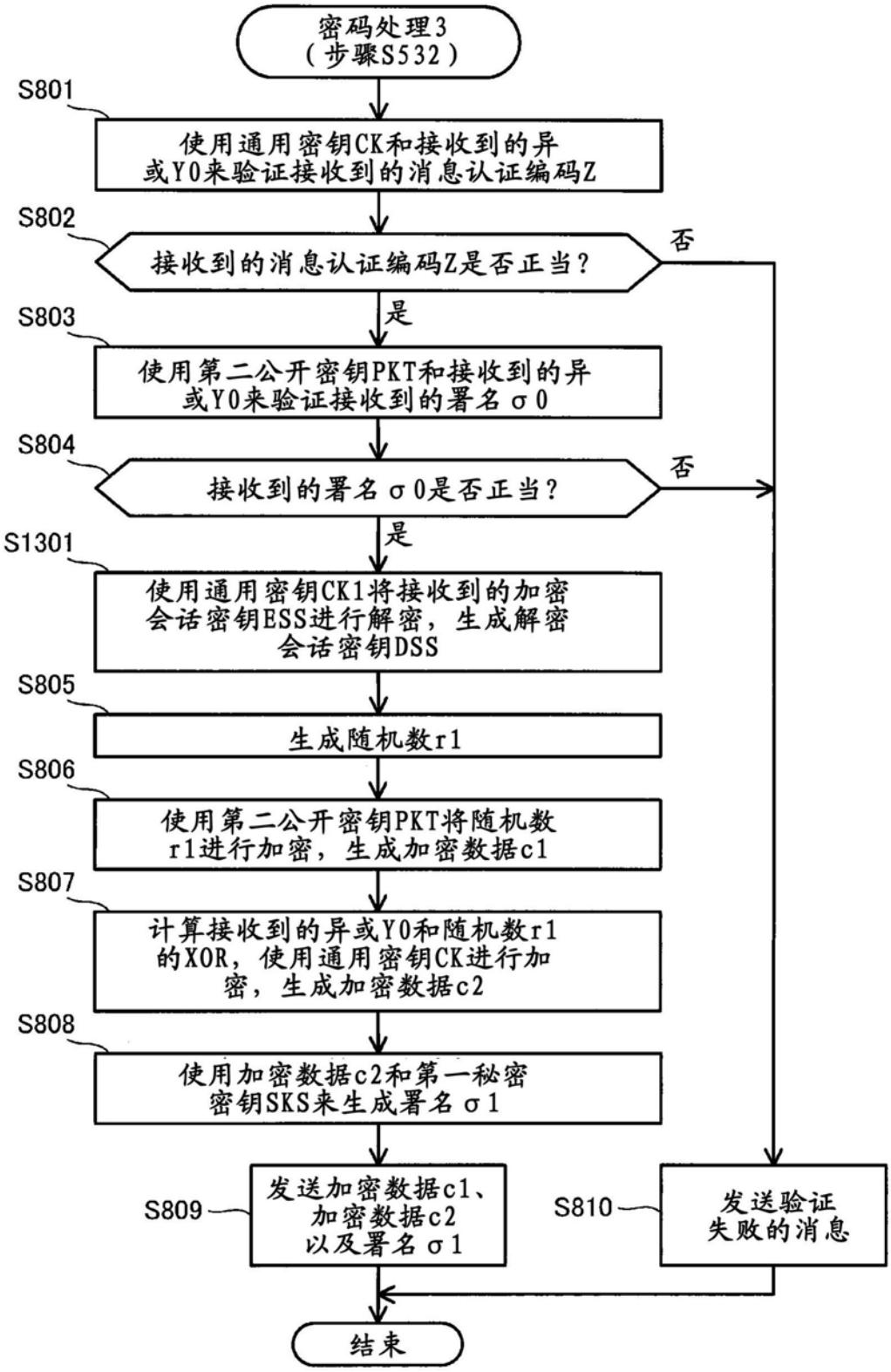

密码处理3
（步骤S532）
S801
使用通用密钥CK和接收到的异或Y0来验证接收到的消息认证编码Z
S802
接收到的消息认证编码Z是否正当？
否
是
S803
使用第二公开密钥PKT和接收到的异或Y0来验证接收到的署名σ0
S804
接收到的署名σ0是否正当？
否
是
S1301
使用通用密钥CK1将接收到的加密会话密钥ESS进行解密，生成解密会话密钥DSS
S805
生成随机数r1
S806
使用第二公开密钥PKT将随机数r1进行加密，生成加密数据c1
S807
计算接收到的异或Y0和随机数r1的XOR，使用通用密钥CK进行加密，生成加密数据c2
S808
使用加密数据c2和第一秘密密钥SKS来生成署名σ1
S809
发送加密数据c1、加密数据c2以及署名σ1
S810
发送验证失败的消息
结束

图15