

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

B60R 25/10 (2006.01)

B60R 16/02 (2006.01)



# [12] 发明专利申请公开说明书

[21] 申请号 200480016379.X

[43] 公开日 2006年7月19日

[11] 公开号 CN 1805870A

[22] 申请日 2004.6.11

[21] 申请号 200480016379.X

[30] 优先权

[32] 2003.6.12 [33] JP [31] 167728/2003

[86] 国际申请 PCT/JP2004/008191 2004.6.11

[87] 国际公布 WO2004/110832 日 2004.12.23

[85] 进入国家阶段日期 2005.12.12

[71] 申请人 株式会社电装

地址 日本爱知县

[72] 发明人 小木曾治比古

[74] 专利代理机构 永新专利商标代理有限公司

代理人 王 英

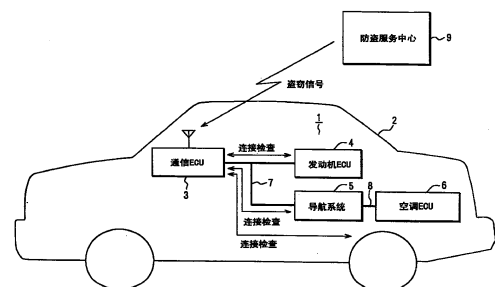
权利要求书 3 页 说明书 11 页 附图 6 页

## [54] 发明名称

防盗系统

## [57] 摘要

本发明的目的是提供一种防盗系统，其能够适当地保护车辆防止被盗。全部安装在车辆 2 中的通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 互相通信以确保电连接或“通信”。当就通信而言检测到异常时，被通信的设备与进行通信检查操作的设备二者都停止工作。如果在车辆 2 被盗的同时任何一个上述设备被从车辆 2 移走，这种操作方案阻止车载设备作为整个系统正确工作。因此，该操作方案大大地降低了盗窃动机，从而适当地保护车辆 2 防止被盗。



1、一种限制对对象的偷盗的防盗系统，该对象具有互相连接的车载设备，其中：

一个所述车载设备执行通信检查操作以用于检查与其余所述车载设备的通信；

当所述一个车载设备检测到所述一个车载设备与其余所述车载设备之间的所述通信正常时，所述一个车载设备使得所述一个车载设备能够进行正常操作并且使得其余所述车载设备能够进行正常操作；以及

当所述一个车载设备检测到所述一个车载设备与其余所述车载设备之间的所述通信异常时，所述一个车载设备停止所述一个车载设备的操作以及其余所述车载设备的操作、或者可选择地使得所述一个车载设备能够进行有限操作并且使得其余所述车载设备能够进行有限操作。

2、如权利要求 1 所述的防盗系统，其中，所有所述车载设备分别执行与其余所述车载设备的所述通信检查操作。

3、如权利要求 2 所述的防盗系统，其中，所述一个车载设备与其余所述车载设备之间的所述通信检查操作是通过对其间通信的数据进行加密而执行的。

4、如权利要求 1 所述的防盗系统，其中所述一个车载设备被设置为控制器并执行与其余所述车载设备的所述通信检查操作。

5、如权利要求 4 所述的防盗系统，其中：

被设置为所述控制器的所述一个车载设备存储多个公有密钥，每个所述公有密钥专用于其余所述车载设备中相应的一个；

其余所述车载设备中的每一个存储自身的专用私有密钥，所述专

用私有密钥与所述自身的专用公有密钥是成对的；以及

被设置为所述控制器的所述一个车载设备与其余所述车载设备之间的所述通信检查操作是通过对其间通信的数据进行加密而执行的，其中通过使用存储在其余所述车载设备中的所述私有密钥和存储在被设置为所述控制器的所述一个车载设备中的所述公有密钥来执行所述数据的加密。

6、如权利要求 4 或 5 所述的防盗系统，其中，被设置为所述控制器的所述一个车载设备具有执行外部通信的通信能力。

7、如权利要求 4 至 6 中任一权利要求所述的防盗系统，其中，被设置为所述控制器的所述一个车载设备基于其余所述车载设备的优先权顺序进行与其余所述车载设备的所述通信检查操作。

8、如权利要求 7 所述的防盗系统，其中：

被设置为所述控制器的所述一个车载设备进行与一个或多个其余所述车载设备的所述通信检查操作；以及

当被设置为所述控制器的所述一个车载设备检测到所述一个车载设备与所述一个或多个其余所述车载设备之间的所述通信正常时，被设置为所述控制器的所述一个车载设备使得所述一个或多个其余所述车载设备能够进行正常操作，然后执行与剩下的一个或多个其余所述车载设备的所述通信检查操作。

9、如权利要求 4 至 8 中任一权利要求所述的防盗系统，其中，被设置为所述控制器的所述一个车载设备以预设的时间间隔执行与其余所述车载设备的所述通信检查操作，所述预设的时间间隔长于预定最小阈值时间间隔且短于预定最大阈值时间间隔。

10、如权利要求 9 所述的防盗系统，其中，当由被设置为所述控制器的所述一个车载设备以长于所述预定最大阈值时间间隔或短于

所述预定最小阈值时间间隔的时间间隔进行所述通信检查操作时，其余所述车载设备停止其自身的操作或执行其自身的有限操作。

11、如权利要求 4 至 10 中任一权利要求所述的防盗系统，其中，当被设置为所述控制器的所述一个车载设备在超过预定时间周期内未执行与其余所述车载设备的所述通信检查操作时，其余所述车载设备请求被设置为所述控制器的所述一个车载设备执行与其余所述车载设备的所述通信检查操作。

## 防盗系统

### 技术领域

本发明涉及一种防盗系统，其防止诸如车辆等的具有互相连接的车载设备的对象被盗。

### 背景技术

广为人知的是，存在一种装置，该装置通过在从防盗服务中心接收到偷盗信号时不允许发动机工作而防止车辆被盗（例如，JP-A-2002-59812）。

然而，可以预见的是，使用现有技术的装置在装置自身被从车辆移走时无法合适地实施用于防止车辆被盗的预期功能，就是说，其无法从防盗服务中心接收到盗窃信号，以便不允许发动机起动。

鉴于上述问题，本发明的防盗系统旨在提供一种系统，该系统能够通过显著减少/降低盗窃动机而适当地防止诸如车辆的具有车载设备的对象被盗。

### 发明内容

在本发明的防盗系统中，诸如车辆的具有车载设备的对象上的设备之一与所述其余车载设备进行通信，以在起动其自身和其余车载设备的操作之前检查电连接。如果没有检查到电连接、或者“通信”，防盗系统停止设备自身和其它设备的操作，或者限制设备自身和其它设备的操作。

因此，如果具有车载设备的对象被盗并且互相连接的车载设备中的任意一个被从该对象移走，那么将检测到一个车载设备和其它设备之间的连接异常。这触发了停止该设备和其它车载设备的操作，或者可选择地实现该设备和其它车载设备的有限操作，并使作为一组设备的整个系统不能正常工作。这样，配备有这样的防盗系统的具有车载

设备的对象通过使盗贼感到不值得偷盗并且降低他/她的盗窃动机，而适当地阻止盗贼偷盗车辆。

在这种情况下，在具有车载设备的对象上的一组车载设备可以与另一组车载设备进行通信，或者在具有车载设备的对象上的每一个设备可以与其它车载设备进行通信以用于通信检查操作。此外，通信检查操作的对象可以是全部车载设备中的一部分或者可以是全部车载设备。此外，有限操作可以仅被施加于在与其它设备的通信检查操作中检测到异常的设备本身，或者可以仅被施加于其它设备。

当分别在所有车载设备之间检查通信时，能够检测到任何通信异常，就是说，由于在被移走的设备和未被移走的设备之间通信失败，所以能够检测到任何被移走的设备。结果，未被移走的设备停止工作，或者未被移走的设备限制其自身的操作，并且将阻止作为系统的一组设备正常工作。在这种情况下，通信检查操作的对象也可以是全部车载设备的一部分或者可以是全部车载设备。

优选地，通过加密通信来检查一个设备与其它设备之间的通信。按照这种方式，能够防止破译通信检查操作步骤，从而能够提高系统的安全性。对称密钥密码术或者公有密钥密码术能够被用于此目的。

可以将一个车载设备设置为控制器来检查与所述其它车载设备的通信。按照这种方式，与每个车载设备互相进行通信的通信检查操作相比，能够简化通信检查操作的控制，从而能够容易地构造系统。

被设置为控制器的一个车载设备持有用于相应设备的公有密钥，并且该相应设备持有与存储在被设置为控制器中的公有密钥相耦合的私有密钥。通过使用这些密钥，就是说，利用所述控制器中的公有密钥和所述相应设备中的私有密钥，能够利用加密通信来执行这两个设备之间的通信检查操作。

按照这种方式，由于所述相应设备持有其自身的私有密钥，因此即使当控制器被移走并且控制器中的公有密钥被解码时，仍然能够安全地对通信检查操作步骤等进行保密，并且能够提高系统的安全性。

被设置为控制器的一个车载设备优选地基于其余车载设备的优先权顺序来检查与其它车载设备的通信。按照这种方式，与某一个车

载设备的通信检查操作能够先于与其余车载设备的通信检查操作而进行。

被设置为控制器的一个车载设备首先检查与其余车载设备中的一部分的通信,然后在检测到与其余车载设备中的一部分的正常通信检查操作并起动其余车载设备中的一部分的操作之后,检查与全部其它车载设备的通信。按照这种方式,例如,能够先于其余的车载设备而检查与发动机 ECU 的通信,这样能够通过检查与其它设备的通信之前起动发动机 ECU,提高了系统的有用性。

被设置为控制器的一个车载设备优选地以预定时间间隔检查与其它车载设备的通信,所述预定时间间隔长于最小阈值且短于最大阈值。当比所需更为频繁地进行通信检查操作时,这可能被盗贼利用而用于破译通信检查操作所用步骤的加密代码。对于这个问题,以长于最小阈值的预定间隔检查通信能够减少盗贼破译通信检查操作步骤的可能性。另外,当比所需更为不经常地检查通信时,当车载设备被从车辆移走时可能给盗贼较长周期来滥用被移走的设备。对于这个问题,以短于最大阈值的预定时间间隔检查通信能够保护被移走的设备使其免于被盗贼在较长时间周期内滥用。

当由被设置为控制器的设备以长于最大阈值的时间间隔或者是以短于最小阈值的时间间隔检查通信时,其它车载设备可以停止其自身的操作或者可以限制其自身的操作。按照这种方式,即使当由于不诚实的动作导致不能正常检查被设置为控制器的设备所进行的通信时,其它车载设备也能够适当地停止其自身的操作或者限制其自身的操作。

优选地,其它设备被规划来使得当被设置为控制器的设备在超过预定时间周期内没有检查通信时,由控制器调用通信检查操作。按照这种方式,系统能够防止其余设备由于没有在预定时间周期内检查与被设置为控制器的设备的通信而被忽视。就是说,例如,能够防止当整个系统的电压下降时,由整个系统的电压下降引起的与其它车载设备的通信检查操作的故障。

## 具体实施方式

### (第一实施例)

参照图 1 到图 4，在这里描述本发明的第一实施例，即本发明在包含车载设备的系统上的应用。第一实施例对应于权利要求 1 至权利要求 3。

图 1 示出整个系统的结构图。防盗系统 1 包括在车辆 2（本发明中具有车载设备的对象）上互相连接的通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6。第一通信线路 7 连接通信 ECU 3、发动机 ECU 4、以及汽车导航系统 5，第二通信线路 8 连接汽车导航系统 5 和空调 ECU 6。

每个那些设备，即通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6，检查与其它车载设备的电连接或“通信”。在这种情况下，通信 ECU 3 通过第一通信线路 7 检查与发动机 ECU 4 的通信。通信 ECU 3 也通过第一通信线路 7 检查与汽车导航系统的通信。此外，通信 ECU 3 还通过第一通信线路 7、汽车导航系统 5 和第二通信线路 8 检查与空调 6 的连接。

按照与上述同样的方式，每个下列设备，即发动机 ECU 4、汽车导航 ECU 5、空调 ECU 6，检查与其它设备的通信。图 2 示出通信检查操作关系以及每个车载设备至控制器的通信检查操作路径的列表。对于通信检查操作，每个下列设备，即通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6，通过使用数据通信来检查通信。当数据通信成功完成时，其被检测到为正常通信，当数据通信没有完成时，其被认为是通信故障。

在上述操作方案中，当车辆 2 处于“被盗”状态时，在通过电话网络接收到盗窃信号后，通信 ECU 3 就向防盗服务中心 9 发送当前位置信号。

接着，参照图 3 和图 4 说明上述方案的操作。在这种情况下，通信 ECU 3 被用作确保与其它设备通信的实例。通信 ECU 3 通过第一通信线路 7 检查与发动机 ECU 4 的通信（步骤 S1）。当通信 ECU 3 检测到与发动机 ECU 4 的成功数据通信时，其确定为通信 ECU 3 与



发动机 ECU 4 之间的通信正常（步骤 S2：是）。

接着，通信 ECU 3 通过第一通信线路 7 检查与汽车导航系统 5 的通信（步骤 S3）。当通信 ECU 检测到与汽车导航系统 5 的成功数据通信时，其确定为通信 ECU 3 与汽车导航系统 5 之间的通信正常（步骤 S4：是）。

接着，通信 ECU 3 通过第一通信线路 7、汽车导航系统 5、以及第二通信线路 8 检查与空调 ECU 6 的通信（步骤 S5）。当通信 ECU 3 检测到与空调 ECU 6 的成功数据通信时，其确定为通信 ECU 3 与空调 ECU 6 之间的通信正常（步骤 S6：是）。

接着，通信 ECU 3 检查与电话网络的通信（S7）。当通信 ECU 3 检测到与电话网络的正常通信时（步骤 S8：是），其确定盗窃信号是否通过电话网络从防盗服务中心 9 接收（步骤 S9）。当通信 ECU 3 检测到不存在从防盗服务中心发送出的盗窃信号时（步骤 S9：否），其输出正常的操作信号以操作发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6（步骤 S10）。

另一方面，当在通信 ECU 3 与发动机 ECU 4 之间的通信中检测到异常时（步骤 S2：否）、或者当在通信 ECU 3 与汽车导航系统 5 之间的通信中检测到异常时（步骤 S4：否）、或者当在通信 ECU 3 与空调 ECU 6 之间的通信中检测到异常时（步骤 S6：否），通信 ECU 3 发送停止操作信号，以便停止发动机 ECU 4、或汽车导航系统 5、或空调 ECU 6 的操作（步骤 S11）。

当在通信 ECU 3 与电话网络之间的通信中检测到异常时（步骤 S8：否）、或者检测到盗窃信号被从防盗服务中心 9 接收到（步骤 S9：是），通信 ECU 3 也输出停止操作信号，以便停止发动机 ECU 4、或汽车导航系统 5、或空调 ECU 6 的操作（步骤 S11）。

通过上述过程，在与这些设备以及与电话网络的通信正常并且不存在从防盗服务中心 9 发送出的盗窃信号的情况下，通信 ECU 3 正常操作发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6。反之，当与设备或与电话网络通信不正常、或者存在从防盗服务中心 9 发送出的盗窃信号时，通信 ECU 停止发动机 ECU 4、汽车导航系统 5、以

及空调 ECU 6 的操作。

在上述情况中，通信 ECU 3 也可以限制发动机 ECU 4、汽车导航系统、以及空调 ECU 6 的操作而不是停止这些设备的操作。此外，当与其它设备的通信正常时，通信 ECU 3 正常操作其自身，并且当与其它设备的通信不正常时，其能够停止其自身的操作或者限制其自身的操作。

下面说明上述通信检查操作的详细内容。在图 4 中，通信 ECU 3 与发动机 ECU 4 之间的通信检查操作步骤被作为典型情况。

通信 ECU 3 产生随机数 X1（步骤 T1），并向发动机 ECU 4 发送包括随机数 X1 的信号 m1。在接收到来自通信 ECU 3 的信号 m1 后，发动机 ECU 4 就从信号 m1 提取随机数 X1，并对随机数 X1 进行加密，从而产生随机数 X2（步骤 T2），并产生随机数 Y1（步骤 T3）。接着，发动机 ECU 4 向通信 ECU 3 发送包括随机数 X2 和 Y1 的信号 m2。

在接收到来自发动机 ECU 4 的信号 m2 后，通信 ECU 3 就从信号 m2 提取随机数 X2 和 Y1，并通过辨别随机数 X2 来确定是否在发动机 ECU 4 中正常执行加密（步骤 T4）。当通信 ECU 3 检测到在发动机 ECU 4 中的正常加密时，其对随机数 Y1 进行加密以产生随机数 Y2（步骤 T5），并向发动机 ECU 4 发送包括随机数 Y2 的信号 m3。

在接收到来自通信 ECU 3 的信号 m3 后，发动机 ECU 4 就从信号 m3 提取随机数 Y2，并通过辨别随机数 Y2 来确定是否在通信 ECU 3 中正常执行加密（步骤 T6）。当发动机 ECU 4 检测到在通信 ECU 3 中的正常加密时，其向通信 ECU 3 发送信号 m4。通信 ECU 3 通过从发动机 ECU 4 接收到信号 m4，检测到与发动机 ECU 4 的正常的数据通信，这样就完成了通信 ECU 3 与发动机 ECU 4 之间的通信检查操作。

在上述步骤中，通过对数据通信进行加密，通信 ECU 3 检查与发动机 ECU 4 的通信，其按照同样的方式通过对数据通信进行加密来检查与汽车导航系统 5 和空调 ECU 6 的通信。按照同样的方式通过对数据通信进行加密来执行其它设备之间的通信检查操作。

当随机数 X1 和 Y1 在每次通信检查操作中被随机产生时，它们能够有效地对用于通信检查操作的数据进行加密。更确切地说，当通信 ECU 3 和发动机 ECU 4 在其存储器中存储多个随机数，并在每一次通信检查操作会话中互相告知它们使用的随机数时，就能够实现上面的方案。另一种确定随机数的方法是在非易失存储器中保存预定的随机数序列并且根据通信 ECU 3 和发动机 ECU 4 之间的顺序取回随机数。

在本发明的第一实施例中，防盗系统的操作方案被规划来使得当在由车辆 2 的每个车载设备进行的通信检查操作处理中检测到异常时，停止另一个设备的操作，所述车辆 2 的每个车载设备即通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6。当车辆 2 被盗并且一个车载设备被移走时，车载设备的整个系统将被阻止正常工作。结果，这使得盗贼认为不值得偷盗，从而将大大减少盗窃动机。那样相应地以适当的方法保护车辆 2 防止被盗。另外，利用车载设备之间的通信检查操作的加密数据保护了通信检查操作步骤，从而提高了防盗系统的安全性。

#### （第二实施例）

接着，参照图 5 和图 6 描述本发明的第二实施例。在这个描述中，省略了与在第一实施例中描述的相同的部分，并且仅描述区别。第二实施例对应于权利要求 1、4 和 11。

在第一实施例中，每个下列设备，即通信 ECU 3、发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6，被规划来确保与其它设备的通信。在第二实施例中，通信 ECU 3 检查与发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 的通信，并且排除了由发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 进行的通信检查操作。换句话说，通信 ECU 3 被规划为本发明的控制设备。

在这个操作方案中，通信 ECU 3 首先确定车辆 2 是否处于被盗状态（步骤 S21）。如果车辆被确定为未处于被盗状态（步骤 S21：否），通信 ECU 3 检查与发动机 ECU 4 的通信（步骤 S22）。当与发动机

ECU 4 的通信检查操作被确定为正常时（步骤 S23：是），在检查与汽车导航系统 5 和空调 ECU 6 的通信之前，通信 ECU 3 向发动机 ECU 4 输出正常操作信号以操作发动机 ECU 4（步骤 S24）。

接着，通信 ECU 3 检查与汽车导航系统 5 的通信（步骤 S25）。当与汽车导航系统的通信检查操作被确定为正常时（步骤 S26：是），通信 ECU 3 检查与空调 ECU 6 的通信（步骤 S27）。当与空调 ECU 6 的通信检查操作被确定为正常时（步骤 S28：是），通信 ECU 3 检查与电话网络的通信（步骤 S29）。

当与电话网络的通信检查操作被确定为正常时（步骤 S30：是），通信 ECU 3 确定盗窃信号是否通过电话网络被从防盗服务中心 9 接收到（步骤 S31）。当没有从防盗服务中心 9 接收到盗窃信号时（步骤 S31：否），通信 ECU 3 向汽车导航系统 5 和空调 ECU 6 输出正常的操作信号以操作这些设备（步骤 S32），并记录为车辆 2 未处于被盗状态（步骤 S33）。

反之，当车辆 2 被确定为处于被盗状态时（步骤 S21：是），通信 ECU 3 进行与在第一实施例中描述的步骤 S1 至步骤 S11 相对应的步骤 S34 至步骤 S44 的处理，并记录为车辆 2 处于被盗状态。

通过执行上述处理，当与发动机 ECU 4 的通信检查操作被确定为正常时，在检查与汽车导航系统 5 和空调 ECU 6 的通信之前，通信 ECU 3 使用不同于第一实施例中使用的方案来起动发动机 ECU 4 的操作。按照这种方式，能够首先立刻起动发动机 ECU 4。

在第二实施例中，通过对数据通信进行加密来检查通信。如图 6 中所示，通信 ECU 3 持有用于发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 的专用公有密钥，且相应的私有密钥由发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 持有。当检查完与发动机 ECU 4 的通信时，通信 ECU 3 使用用于发动机 ECU 4 的专用公有密钥对数据进行编码并将其发送到发动机 ECU 4。发动机 ECU 4 通过使用用于发动机 ECU 4 的相应私有密钥，解密来自通信 ECU 3 的数据。

在第二实施例中，通信 ECU 3 被规划来确保以长于最小阈值且短于最大阈值的预定时间间隔与其它车载设备进行通信。在这种情况下

下,可以由系统自身或者可以由系统的用户来确定预定时间间隔的下限和上限。当以长于最大阈值或短于最小阈值的时间间隔检查通信时,通信检查操作的时机异常,每个下列设备,即发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6,被规划来停止其自身的操作或限制其自身的操作。

此外,发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 被规划来使得当由通信 ECU 3 检查的通信在预定时间周期内没有起动机时,能够确保通信。在这种情况下,预定时间周期可以由系统自身定义或者可以由系统的用户确定。

如上所述,在车辆 2 上的车载设备当中,在系统的第二实施例中,通信 ECU 3 检查与诸如发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 的其它设备的通信。当在通信检查操作过程中检测到异常时,系统被规划来停止其它车载设备的操作。因此,如果任一车载设备被从处于被盗状态的车辆 2 移走,该操作方案阻止系统作为一组设备正常工作。结果,盗贼认为不值得偷盗车辆 2,且盗窃的动机将被降低,从而适当地保护车辆 2 以免被盗。

当仅仅通信 ECU 3 被规划来确保与其它车载设备的通信时,与第一实施例中的操作方案相比,能够简化且容易地构造防盗系统的控制,所述其它车载设备即发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6。

此外,通信 ECU 3 持有用于每一个其它车载设备的专用公有密钥,且发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 持有其自身的私有密钥,系统被规划来通过使用这些公有密钥和私有密钥对数据通信进行加密来确保通信。因此,即使当通信 ECU 3 被从车辆 2 移走且通信 ECU 3 的公有密钥被解密时,由于加密的私有密钥由其它车载设备持有,所以系统的安全性得到提高且通信检查操作步骤无法被容易地解密。

当与发动机 ECU 4 的通信检查操作被确定为正常时,在检查与汽车导航系统 5 和空调 ECU 6 的通信之前,通信 ECU 3 向发动机 ECU 4 输出正常操作信号以操作发动机 ECU 4。这个操作方案使系统首先

立刻起动发动机 ECU 4 并且系统的有用性得到提高。

此外，通信 ECU 3 被规划来确保以长于最小阈值且短于最大阈值的预定时间间隔与其它车载设备进行通信。当比所需更为频繁地检查通信时，可能被盗贼利用来破译通信检查操作所用步骤的加密代码。对于这个问题，以长于最小阈值的预定时间间隔检查通信能够减少由盗贼破译通信检查操作步骤的可能性。另外，当比所需更为不经常地检查通信时，当车载设备被从车辆 2 移走时可能使盗贼在较长时间周期内使用被移走的设备。对于这个问题，以短于最大阈值的预定时间间隔检查通信能够防止盗贼滥用被移走的设备。

此外，当由通信 ECU 3 以长于预定最大时间周期的间隔或者是以短于最小预定时间周期的间隔检查通信时，诸如发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 的设备被规划来停止其自身操作或者限制其自身操作。按照这种方式，即使当由于不诚实动作导致通信 ECU 3 不能正常执行通信检查操作时，发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 也能够适当地停止其自身的操作或者限制其自身的操作。

此外，发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6，被规划来使得在预定时间周期内没有检查通信时，由通信 ECU 3 调用通信检查操作。按照这种方式，系统能够防止发动机 ECU 4、汽车导航系统 5、以及空调 ECU 6 由于没有在预定时间周期内检查通信而被忽视。

### （第三实施例）

接着，参照图 7 描述第三实施例。省略了与在第二实施例中描述过的相同的部分，仅描述区别。在第二实施例中，仅仅是通信 ECU 3 作为控制设备正在检查通信。在第三实施例中，通信 ECU 3 和发动机 ECU 4 都被当作控制设备以确保通信。

在这种情况下，通信 ECU 3 和发动机 ECU 4 二者都将控制汽车导航系统 5 和空调 ECU 6，且汽车导航系统 5 和空调 ECU 6 的受限操作的程度将由一种策略确定，所述策略是较大限制覆盖较小限制。

因此，即使当由于内部结构的暴露导致通信 ECU 3 不能被用作控制设备时，发动机 ECU 4 还能作为控制设备工作，从而能够如第一和第二实施例中所描述的那样阻止车载设备正常操作。结果，这种操作方案使盗贼认为不值得偷盗车辆且降低了盗窃的动机，适当地保护了车辆防止被盗。

#### （其它实施例）

本发明并不限于上面的实施例，而是可以如下面一样修改或增强。

所述操作方案不仅可用于车辆的车载设备，而且可用于装在其它类型装置上的设备。

当在每个设备中安装通信检查操作功能时，也可以将这些设备之间连接的电汽配线（wire-harness）修改为具有特有结构以容纳不同数量的信号等。按照这种方式，通过降低盗窃的动机，电汽配线的专有结构适当地防止了车辆 2 被盗，且当车辆 2 被盗时车载设备被从车辆 2 移走时，损害的扩散也能够得到抑制。

#### 附图简述

图 1 示出本发明的第一实施例的示意图；

图 2 示出表示与作为通信检查操作的对象每个车载设备的连接的设备 and 这些设备的通信检查操作路径的图；

图 3 示出表示通信 ECU 3 如何检查与其它车载设备的通信的流程图；

图 4 示出表示通信 ECU 3 如何检查与发动机 ECU 4 的通信的流程图；

图 5 示出表示本发明的第二实施例的流程图；

图 6 示出每个车载设备的公有密钥和私有密钥；

图 7 示出表示控制设备、连接的设备（通信检查操作的对象）和受控设备之间的关系图。

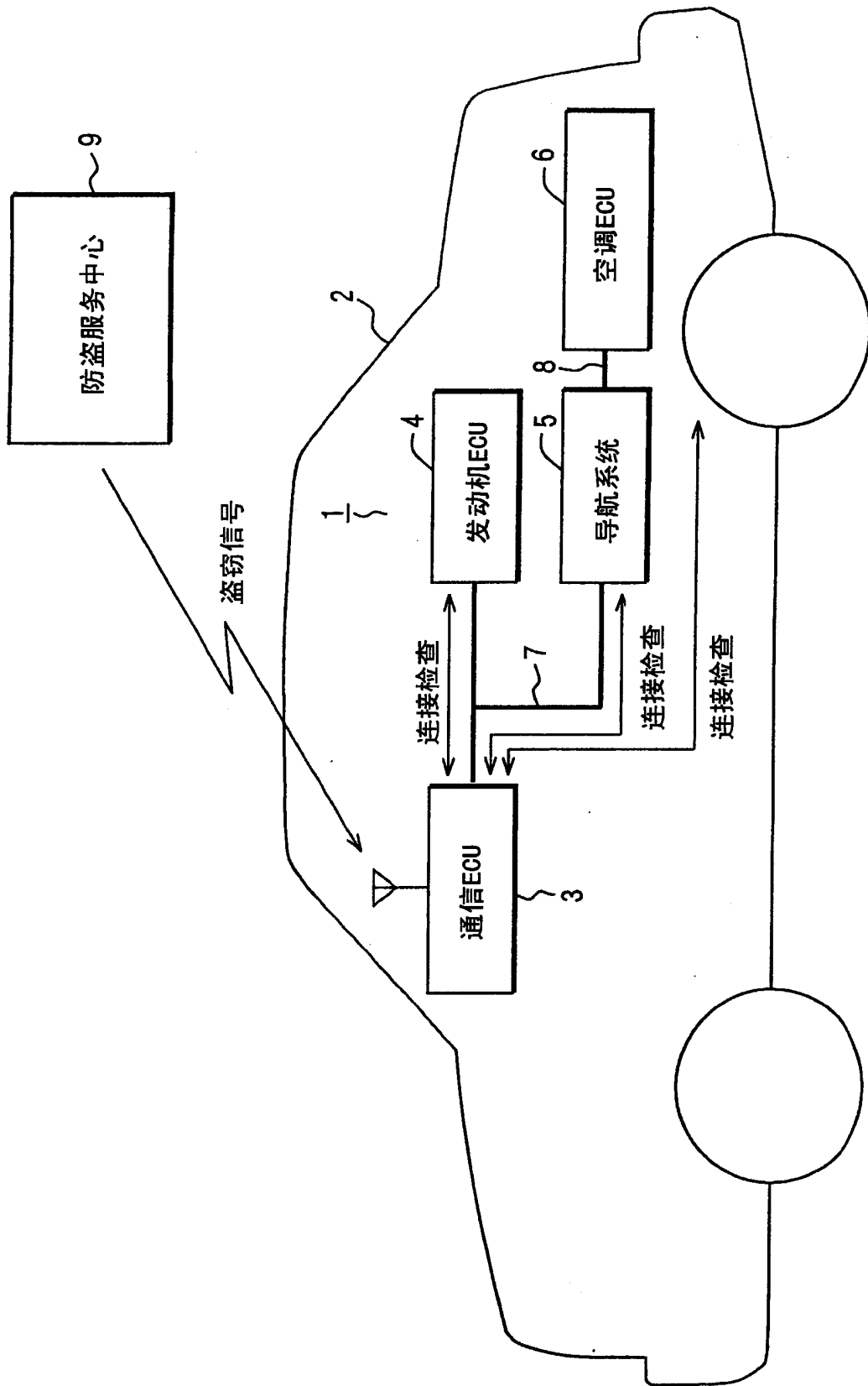


图1



| 设备名称   | 通信检查的设备 | 连接检查路径               |
|--------|---------|----------------------|
| 通信ECU  | 发动机ECU  | 第一通信线路               |
|        | 汽车导航系统  | 第一通信线路               |
| 发动机ECU | 空调ECU   | 第一通信线路—汽车导航系统—第二通信线路 |
|        | 通信ECU   | 第一通信线路               |
|        | 汽车导航系统  | 第一通信线路               |
|        | 空调ECU   | 第一通信线路—汽车导航系统—第二通信线路 |
| 汽车导航系统 | 通信ECU   | 第一通信线路               |
|        | 发动机ECU  | 第一通信线路               |
|        | 空调ECU   | 第二通信线路               |
| 空调ECU  | 通信ECU   | 第二通信线路—汽车导航系统—第一通信线路 |
|        | 发动机ECU  | 第二通信线路—汽车导航系统—第一通信线路 |
|        | 汽车导航系统  | 第二通信线路               |

图2

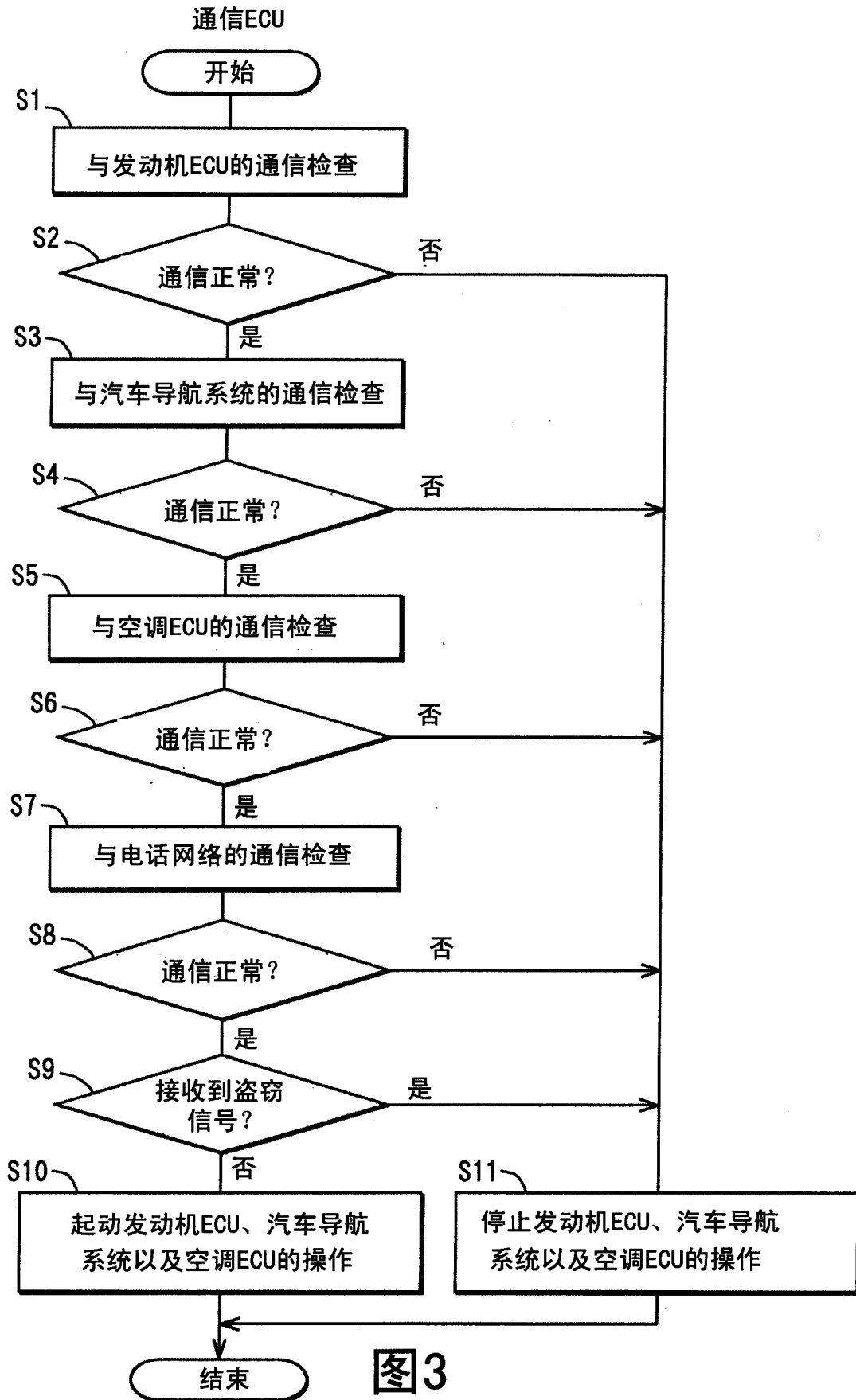


图3

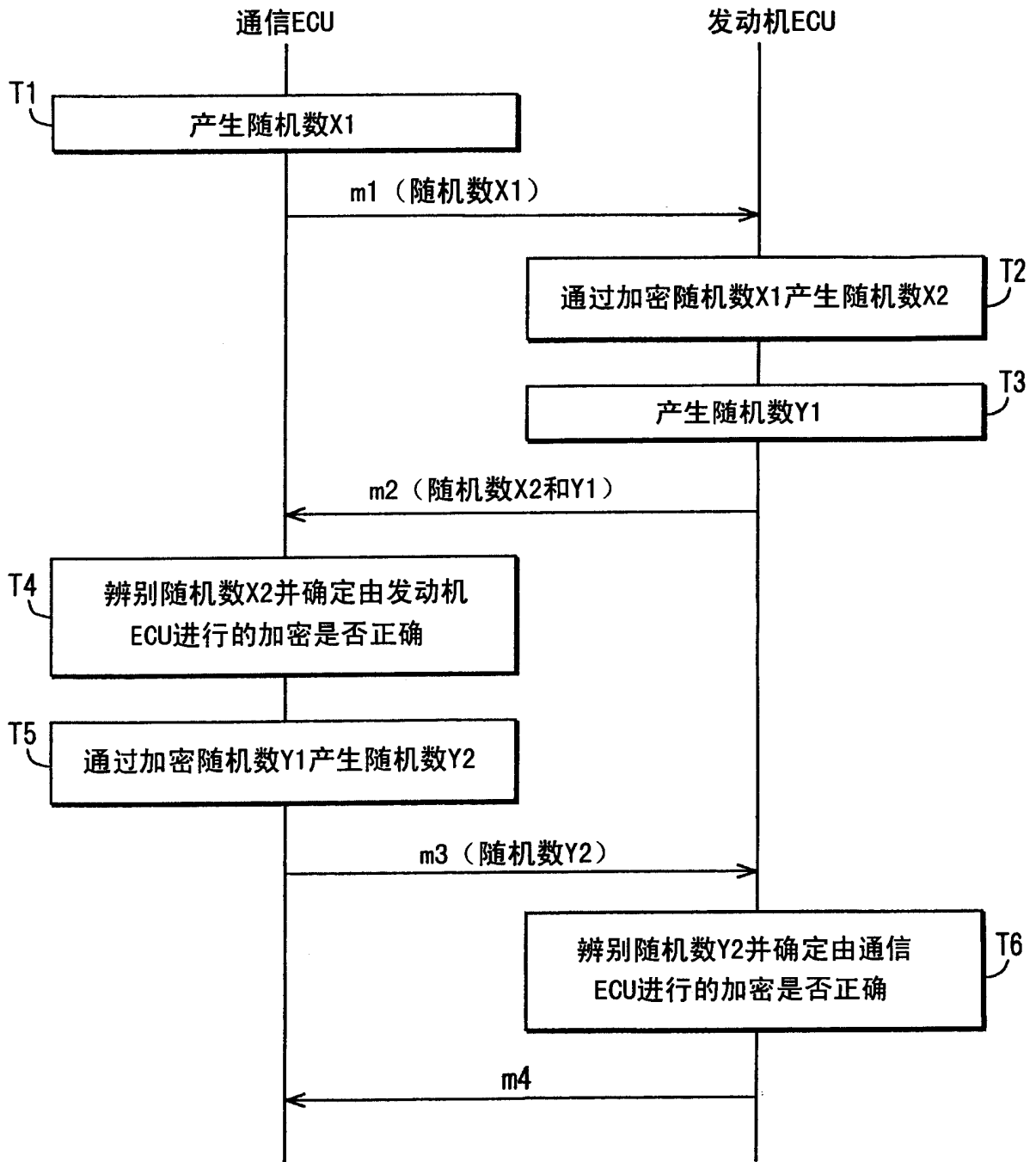


图4

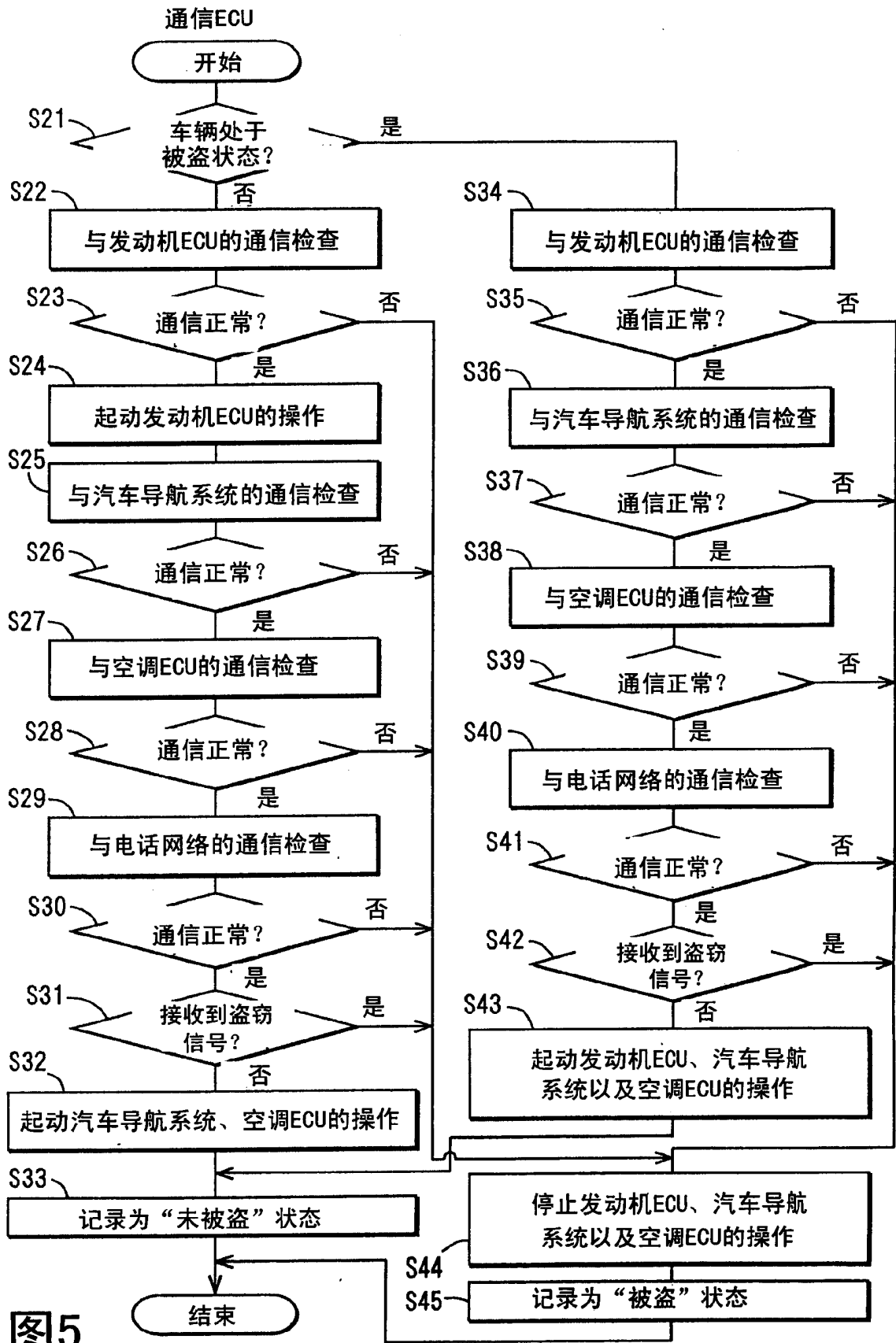


图5

| 设备名称   | 加密密钥和解密密钥   |
|--------|---|
| 通信ECU  | 专用于发动机ECU的公有密钥<br>专用于汽车导航系统的公有密钥<br>专用于空调ECU的公有密钥 |
| 发动机ECU | 专用于发动机ECU的私有密钥                                    |
| 汽车导航系统 | 专用于汽车导航系统的私有密钥                                    |
| 空调ECU  | 专用于空调ECU的私有密钥                                     |

图6

| 控制器    | 通信检查的设备   | 受控设备   |
|--------|---|--|
| 通信ECU  | <ul style="list-style-type: none"> <li>· 发动机ECU</li> <li>· 汽车导航系统</li> <li>· 空调ECU</li> </ul> | <ul style="list-style-type: none"> <li>· 通信ECU</li> <li>· 发动机ECU</li> <li>· 汽车导航系统</li> <li>· 空调ECU</li> </ul> |
| 发动机ECU | <ul style="list-style-type: none"> <li>· 通信ECU</li> <li>· 汽车导航系统</li> <li>· 空调ECU</li> </ul>  | <ul style="list-style-type: none"> <li>· 通信ECU</li> <li>· 发动机ECU</li> <li>· 汽车导航系统</li> <li>· 空调ECU</li> </ul> |

图7