



## (12)发明专利

(10)授权公告号 CN 104704792 B

(45)授权公告日 2018.05.01

(21)申请号 201380052680.5

(22)申请日 2013.09.27

(65)同一申请的已公布的文献号  
申请公布号 CN 104704792 A

(43)申请公布日 2015.06.10

(30)优先权数据  
102012218488.0 2012.10.10 DE

(85)PCT国际申请进入国家阶段日  
2015.04.09

(86)PCT国际申请的申请数据  
PCT/EP2013/070195 2013.09.27

(87)PCT国际申请的公布数据  
W02014/056731 DE 2014.04.17

(73)专利权人 大陆汽车有限责任公司  
地址 德国汉诺威

(72)发明人 S·勒梅尔勒 U·施特林

(74)专利代理机构 北京市中咨律师事务所  
11247

代理人 吴鹏 马江立

(51)Int.Cl.  
H04L 29/06(2006.01)  
H04L 29/08(2006.01)

(56)对比文件  
US 7979706 B1,2011.07.12,  
WO 2012038185 A1,2012.03.29,  
CN 102035874 A,2011.04.27,  
CN 102035874 A,2011.04.27,

审查员 李珍珍

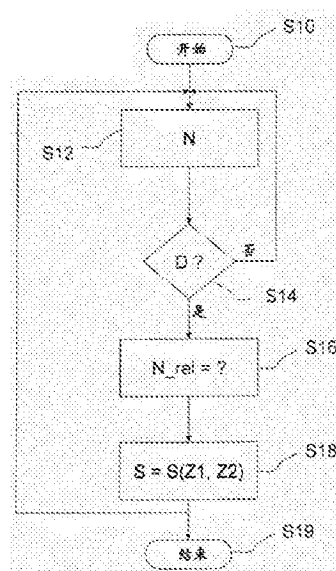
权利要求书1页 说明书5页 附图3页

### (54)发明名称

用于运行车辆的应用的方法和装置

### (57)摘要

在根据本发明的方法中,基于车对X消息(N)的预先规定的信息,将相应的接收到的车对X消息(N)至少部分地传递给车辆的至少一个应用(30)。在此,车对X消息(N)包含数字签名。基于一决定信号(D)来验证对于所述行动的执行而言是与决定相关的车对X消息(N\_rel)的数字签名,该决定信号响应于车对X消息(N)向所述至少一个应用(30)的传递而被提供并且表明车对X消息(N)是否包含引发执行预先规定的的应用(30)行动的数据。此外,基于数字签名的验证的结果提供信号(S),该信号表明与决定相关的车对X消息(N\_rel)的可靠性。



1. 一种用于运行至少一个用于车辆的应用 (30) 的方法, 所述车辆具有通信设备, 所述通信设备配置成从其他车辆接收预先规定的车对X消息 (N), 其中

- 基于车对X消息 (N) 的预先规定的信息, 将相应的接收到的车对X消息 (N) 至少部分地传递给所述至少一个应用 (30), 其中, 车对X消息 (N) 包含数字签名,

- 基于一决定信号 (D) 来验证对于预先规定的车辆行动的执行而言是与决定相关的车对X消息 (N\_rel) 的数字签名, 该决定信号响应于车对X消息 (N) 向所述至少一个应用 (30) 的传递而被提供并且表明车对X消息 (N) 是否包含引发执行预先规定的应用 (30) 的车辆行动的数据, 预先规定的车辆行动是能够被车辆驾驶员识别到的车辆功能,

- 基于数字签名的验证的结果提供信号 (S), 该信号表明与决定相关的车对X消息 (N\_rel) 的可靠性,

- 验证与决定相关的车对X消息 (N\_rel),

- 为所述预先规定的车辆行动分配紧迫性, 并且, 基于车辆行动的紧迫性执行以下操作之一:

(a) 在执行预先规定的应用 (30) 的车辆行动的过程中, 验证与决定相关的车对X消息 (N\_rel) 并且产生信号 (S), 基于产生的信号 (S) 终止预先规定的车辆行动, 和

(b) 在执行预先规定的应用 (30) 的车辆行动之前, 验证与决定相关的车对X消息 (N\_rel) 并且产生信号 (S)。

2. 根据权利要求1所述的方法, 其中, 预先规定所述紧迫性。

3. 根据权利要求1所述的方法, 其中, 基于至少一个所述与决定相关的车对X消息 (N\_rel) 确定所述紧迫性。

4. 根据权利要求1所述的方法, 其中, 一旦与决定相关的车对X消息 (N\_rel) 中的一个被归类为不可靠, 就将验证视作已结束并且提供信号 (S)。

5. 根据权利要求1所述的方法, 其中, 当与决定相关的车对X消息 (N\_rel) 的总数目超出上限值时, 以抽样方式对与决定相关的车对X消息 (N\_rel) 进行验证。

6. 根据权利要求1所述的方法, 其中, 基于在预先规定的时间跨度内接收到的车对X消息 (N) 的数目, 验证一个或多个特殊的车对X消息的数字签名然后将一个或多个特殊的车对X消息 (N\_spe) 分别分配给所述至少一个应用 (30), 其中, 基于至少一个预先规定的标准将相应的车对X消息 (N) 归类为特殊的车对X消息 (N\_spe)。

7. 根据权利要求1所述的方法, 其中, 当同时或者在预先规定的时间跨度内提供了多个决定信号 (D) 时,

- 基于预先规定的规则为相应的车辆行动相应确定行动优先级, 和

- 基于相应确定的行动优先级来验证车辆行动的相应的与决定相关的车对X消息 (N\_rel)。

## 用于运行车辆的应用的方法和装置

### 技术领域

[0001] 本发明涉及一种用于运行车辆的应用的方法和装置,和一种具有该装置和应用的车辆系统。

### 背景技术

[0002] 在车对车通信和车对基础设施通信中,车辆与其他车辆或者与基础设施设备通信。该通信还被统称为车对X通信(V2X通信)。这种类型的V2X系统尤其起到为在车辆的驾驶员辅助系统和/或安全系统中的应用交换数据的作用。面临的问题是要确保所传递的车对X信息的必要的数据真实性,因为这些信息还能够被用作对车辆控制进行干预的基础。因此错误的或最严重时甚至是伪造的车对X信息会造成严重后果,必须被可靠地识别为不可信的。

### 发明内容

[0003] 本发明的目的是,提供一种用于运行用于车辆的应用的方法和一种相应的装置,以及一种车辆系统,所述方法、相应的装置以及车辆系统有助于提高在车辆中执行应用的效率和/或可靠性。

[0004] 该目的通过独立权利要求的特征得以实现。本发明的有利的改进方案在从属权利要求中体现。

[0005] 按照本发明的第一和第二方面,本发明的特征在于一种用于运行用于车辆的至少一个应用的方法和一种相应的装置。在此,基于车对X消息的预先规定的信息,将相应的接收到的车对X消息至少部分地传递给所述至少一个应用。在此,车对X消息包含数字签名。基于一决定信号来验证对于所述行动的执行而言是与决定相关的车对X消息的数字签名,该决定信号响应于车对X消息向所述至少一个应用的传递而被提供并且表明车对X消息是否包含引发执行预先规定的应用行动的数据。此外,基于数字签名的验证的结果提供信号,该信号表明与决定相关的车对X消息的可靠性。

[0006] 其优点在于,可以为车对X通信使用公钥基础设施(PKI)。可以使用密码算法。

[0007] 车对X消息分别具有数字签名。尤其有利的是,由相应的应用来决定是否使用车对X消息,并且可以基于接收到的车对X消息与该车辆是否实际相关来验证车对(X)消息。这样的优点是,无需对所有接收到的车对X消息的数字签名都进行验证。由此可以节省计算能力并且降低设计用于执行数字签名验证的安全设备的制造成本。此外这样还有助于提高车对X消息可信性识别的可靠性,因为能够有更多的计算能力被用于更快和/或更准确地进行检验。

[0008] 车辆的相应的应用可以包括车辆的驾驶员辅助系统和/或安全系统和/或舒适系统。在此,相应的行动可以尤其包括能够被车辆使用者识别到的相应的车辆功能,例如对驾驶员的信息通知、警报信号通知、对车辆行驶动力的干预等等。

[0009] 在所述第一和第二方面的一种有利的实施方案中,在执行预先规定的应用行动之

前,验证与决定相关的车对X消息并且提供信号,基于该信号启动预先规定的应用行动的执行。这样以有利的方式使得能够在执行预先规定的行动之前,验证并进而检查与决定相关的车对X消息的可信性。这一点可以被有利地用于尤其是与车辆安全有关的行动。

[0010] 在按照所述第一和第二方面的另一有利的实施方案中,在执行预先规定的行动的过程中,验证与决定相关的车对X消息并且提供信号,基于提供的信号终止至少一个预先规定的应用行动的执行。这一点以有利的方式使得早在执行预先规定的行动的过程中就能够验证并进而检查与决定相关的车对X消息的可信性。这一点可以有利地被用于时间非常紧迫并需要快速反应的行动。

[0011] 在按照所述第一和第二方面的另一种有利的实施方案中,为所述预先规定的行动分配紧迫性,并且基于行动的紧迫性,要么在启动预先规定的应用行动之前,要么在执行预先规定的应用行动的过程中,验证与决定相关的车对X消息和产生信号。通过紧迫性的分配可以简单预先规定所述行动中的哪些行动是时间非常紧迫的,哪些则不是。这一点使得能够简单决定是要在执行相应行动之前、还是在执行该行动的过程中进行验证。

[0012] 在根据第一和第二方面的另一有利的实施方案中,预先规定所述紧迫性。这使得能够实现对相应行动的相应的紧迫性的简单评估,并因此非常快速决定是要在执行相应行动之前、还是要在执行该行动的过程中进行验证。

[0013] 在根据第一和第二方面的另一有利的实施方案中,基于至少一个所述与决定相关的车对X消息确定所述紧迫性。这样做的优势是,能够即时确定紧迫性。所述相应的与决定相关的车对X消息可以包含预先规定了执行预先规定的行动的可能的反应时间的用户数据、例如表明距碰撞的时间长度(碰撞时间,TTC)的用户数据。

[0014] 在根据第一和第二方面的另一有利的实施方案中,一旦与决定相关的车对X消息中的一个被归类为不可靠,就将验证视作已结束并且提供信号。这样可以有利地保持小的验证时间长度。一旦与决定相关的车对X消息中的一个被归类为不可信并因此被归类为不可靠,那么就可以中断验证并且不启动或者终止相应行动的执行。

[0015] 在根据第一和第二方面的另一有利的实施方案中,当与决定相关的车对X消息的总数目超出上限值时,以抽样方式对与决定相关的车对X消息进行验证。这一点以有利的方式使得能够快速地对与决定相关的车对X消息作出验证。这一点可以特别有利地被用于与决定相关的车对X消息的总数目非常大的情况,例如在大量车辆发出的堵车警报的情况下。

[0016] 在根据第一和第二方面的另一有利的实施方案中,基于在预先规定的时间跨度内接收到的车对X消息的数目,验证一个或多个特殊的车对X消息的数字签名然后将一个或多个特殊的车对X消息分别分配给所述至少一个应用,其中,基于至少一个预先规定的标准将相应的车对X消息归类为特殊的车对X消息。这一点可以非常有利地用于当设计用于执行数字签名验证的安全设备的计算容量未被完全或非常高程度地利用的情况。在此情况下,在将这些特殊的车对X消息分配给相应的应用之前,并且在将其归类为与决定相关之前,就可以验证这些特殊的车对X消息的数字签名。这使得当将相应的特殊的车对X消息用于决定是否执行相应的预先规定的行动时,不需要再对其进行验证。

[0017] 在根据第一和第二方面的另一种有利的实施方案中,当同时或者在预先规定的时间跨度内提供了多个决定信号时,基于预先规定的规则分别为相应的行动确定行动优先级,和基于所分别确定的行动优先级来验证行动的相应的与决定相关的车对X消息。这一点

以有利的方式使得当多个应用同时或近似同时决定要执行一个预先规定的应用时,基于相应的行动优先级能够确定究竟要执行哪些行动和/或以哪种顺序来执行相应的行动。

[0018] 按照第三方面,本发明的特征是一种车辆系统,该车辆系统具有根据第二方面的装置和车辆的预先规定的应用,其中,应用设计用于基于至少部分地传递给应用的车对X消息来决定是否执行应用的至少一个预先规定的行动。此外该应用设计用于为所述装置提供决定信号,该决定信号表明车对X消息包含了引发执行应用的预先规定行动的数据。此外所述应用设计用于基于由装置所产生的、表明与决定相关的车对X消息的可靠性的信号来控制所述至少一个预先规定的行动的执行。

[0019] 所述第一和第二方面的有利的实施方案在此也适用于第三方面。

## 附图说明

[0020] 下面借助示意图详述本发明的实施例。附图示出:

[0021] 图1示出车辆系统的框图,

[0022] 图2示出用于运行应用的第一程序的示例性流程图,和

[0023] 图3示出用于运行应用的第二程序的示例性流程图。

[0024] 在所有附图中,具有同样构造或功能的元件以相同的附图标记标出。

## 具体实施方式

[0025] 图1示出了车辆系统10的实施例。

[0026] 车辆系统10具有用于车辆的应用30和用于运行该应用30的装置20。该装置20在该实施例中分配有通信设备22。作为备选方案,装置20也可以具有通信设备22。

[0027] 装置20可以具有专门的车辆控制装置或者车辆的中央计算单元。该装置20与通信设备22通过信号技术连接。通信设备22设计用于从位于车辆的预先规定的周围环境的其他车辆和/或基础设施中接收预先规定的车对X消息N。车对X消息N包含用户数据和安全数据。车对X消息N包含数字签名。这使得能够对车对X消息N的可信性进行检查。数字签名的计算可以例如在椭圆曲线密码算法基础上进行。

[0028] 应用30例如包括驾驶员辅助系统。替代或补充于此,该应用30可以具有车辆的安全系统和/或车辆的舒适系统。所述应用30设计用于基于至少部分地传递给应用30的车对X消息N来决定是否执行应用30的至少一个预先规定的行动。此外该应用30设计用于为装置20提供决定信号D,该决定信号表明车对X消息N包含了引发执行应用30的预先规定行动的数据。此外,应用30设计用于基于由装置20所产生的、表明与决定相关的车对X消息N<sub>rel</sub>的可靠性的信号S来控制所述至少一个预先规定的行动的执行。

[0029] 装置20可以例如设计用于暂存和标识车对X消息N的相应的副本。应用30可以设计用于例如在使用该标识的前提下,通知装置20哪些车对X消息N对于相应的行动而言是与决定相关的,从而使装置20能够对相应行动的与决定相关的车对X消息N<sub>rel</sub>实施签名验证。

[0030] 图2示出了用于运行车辆的应用30的第一程序的示例性流程图。用于运行车辆的应用30的装置20例如具有计算单元以及程序存储器,并被设计用于执行所述第一程序。

[0031] 在图2中所示的流程图中,在步骤S10中启动第一程序。该第一程序可以例如随着车辆激活而启动。

[0032] 在步骤S12中对分别接收到的车对X消息N的相应的预先规定的信息加以评估,并且基于车对X消息N的该预先规定的信息,将车对X消息N至少部分地传递给至少一个应用30。车对X消息N在此包含数字签名。

[0033] 在步骤S14中,检测是否由至少一个应用30提供了决定信号D。还可以同时或近似同时地检测以及由多个应用30提供多个决定信号。

[0034] 在步骤S16中,基于作为对车对X消息N向至少一个应用30传递的答复而提供的、表明车对X消息N是否包含引发执行应用30的预先规定行动的数据的结论的相应的决定信号D来验证对于要执行所述行动而言是与决定相关的车对X消息N\_rel的数字签名。

[0035] 验证在此尤其包括,基于数字签名来检查与决定相关的车对X消息N\_rel是否可信。

[0036] 如果在步骤S16中确定了与决定相关的车对X消息N\_rel是可信的,那么例如在步骤S18中产生并且发出控制信号,该控制信号具有第一状态Z1,其中,该第一状态表明与决定相关的车对X消息N\_rel具有足够的可靠性并且可以执行应用30的预先规定的行动。

[0037] 如果在步骤S16中确定了,与决定相关的车对X消息N\_rel是不可信的,那么例如在步骤S18中产生并且发出控制信号,该控制信号具有第二状态Z2,其中,该第二状态表明与决定相关的车对X消息N\_rel不具有足够的可靠性并且不应该执行应用30的预先规定的行动。

[0038] 优选在步骤S18之后在步骤S12中继续第一程序。在步骤S19中可以结束该程序。

[0039] 在此可以提出,为预先规定的行动分配紧迫性,并基于行动的紧迫性来验证与决定相关的车对X消息N\_rel,并且产生信号S。

[0040] 如果例如所述行动具有低等或中等紧迫性,那么可以在执行应用30的预先规定的行动之前验证与决定相关的车对X消息N\_rel并且提供信号S。基于信号S来启动或不启动应用30的预先规定行动的执行。

[0041] 相反,如果所述行动具有高紧迫性,那么可以在执行预先规定行动的过程中验证与决定相关的车对X消息N\_rel并且提供信号S。基于所提供的信号S来终止应用30的至少一个预先规定的行动的执行或者继续执行。这一点可以有利地用于时间紧迫的、需要尽可能快地做出反应并且不能等待几毫秒的验证时间的行动。这样一种时间紧迫的行动可以例如包括激活报警灯和/或做好刹车准备。验证随着行动的开始同时或近似同时地启动。

[0042] 相应的预先规定行动的紧迫性在此可以是预先规定的或者可以基于至少一个与决定相关的车对X消息N\_rel来确定。

[0043] 此外可以提出,尤其是当逐步和/或按顺序验证与决定相关的车对X消息N\_rel时,一旦与决定相关的车对X消息N\_rel中的一个被归类为不可靠,就将验证视为已结束并且提供信号S。

[0044] 此外可以提出,当对于相应行动存在非常多的与决定相关的车对X消息N\_rel时,分别从大量用于该行动的与决定相关的车对X消息N\_rel中抽样。如果例如抽样验证是成功的,那么执行该行动。在预先规定的下一时间步骤中,对下一抽样进行验证。该过程一直重复,直至应用30结束该行动或者应用30终止。

[0045] 此外可以提出,当同时或者在预先规定的时间跨度内提供了多个决定信号D时,那么基于预先规定的规则为相应的行动相应确定行动优先级,和基于相应确定的行动优先级

来验证行动的相应的与决定相关的车对X消息N<sub>rel</sub>。

[0046] 图3示出了用于运行车辆的应用30的第二程序的示例性流程图。装置20设计用于补充或替代于第一程序来执行该第二程序。

[0047] 第二程序的程序步骤S20、S22、S24、S26、S28和S29在此与第一程序的程序步骤S10至S19相一致。

[0048] 与第一程序不同的是,在第二程序中,在步骤S21中对接收到的车对X消息N的数目和与之相关的装置20的计算负荷的检查进行问询。如果装置20具有足够的计算容量C,那么在步骤S23中,在将一个或多个特殊的车对X消息N<sub>spe</sub>分别分配给至少一个应用30之前,对其数字签名进行验证。如果相应的特殊的车对X消息N<sub>spe</sub>的验证的结果是可信的,那么在步骤S25中,基于预先规定的信息将相应的特殊的车对X消息N<sub>spe</sub>至少部分地传递给相应的应用30。应用30在此情况下设计用于以合适的方式对这些可信的特殊的车对X消息N<sub>spe</sub>加以评估。

[0049] 在此基于至少一个预先规定的标准将相应的车对X消息N归类为特殊的车对X消息N<sub>spe</sub>。特殊的车对X消息N<sub>spe</sub>的这种归类例如可以借助如下标准进行:

[0050] -级别,也就是在预处理中,确定车对X消息N的级别,并基于该顺序将车对X消息N归类为特殊的车对X消息N<sub>spe</sub>;

[0051] -距离,也就是将通知了另一车辆与该车辆之间的最小间距的车对X消息N归类为特殊的车对X消息N<sub>spe</sub>;

[0052] -碰撞时间(TTC),也就是将通知了距碰撞的最小时间的车对X消息N归类为特殊的车对X消息N<sub>spe</sub>;

[0053] -历史,也就是将定期发出的并且在之前的周期中曾涉及过和/或曾与决定相关的车对X消息N归类为特殊的车对X消息N<sub>spe</sub>;

[0054] -标志旗,也就是将具有特殊标志的车对X消息N——例如救护车或紧急制动——归类为特殊的车对X消息N<sub>spe</sub>;

[0055] -消息类型,也就是基于车对X消息N所具有的消息类型将车对X消息归类为特殊的车对X消息N<sub>spe</sub>;在此,可能的消息类型是SPaT(交通灯信号相信息),DENM(分散式环境通知消息)和CAM(协同感知消息)。尤其是还可以基于消息类型预先规定评估的顺序。

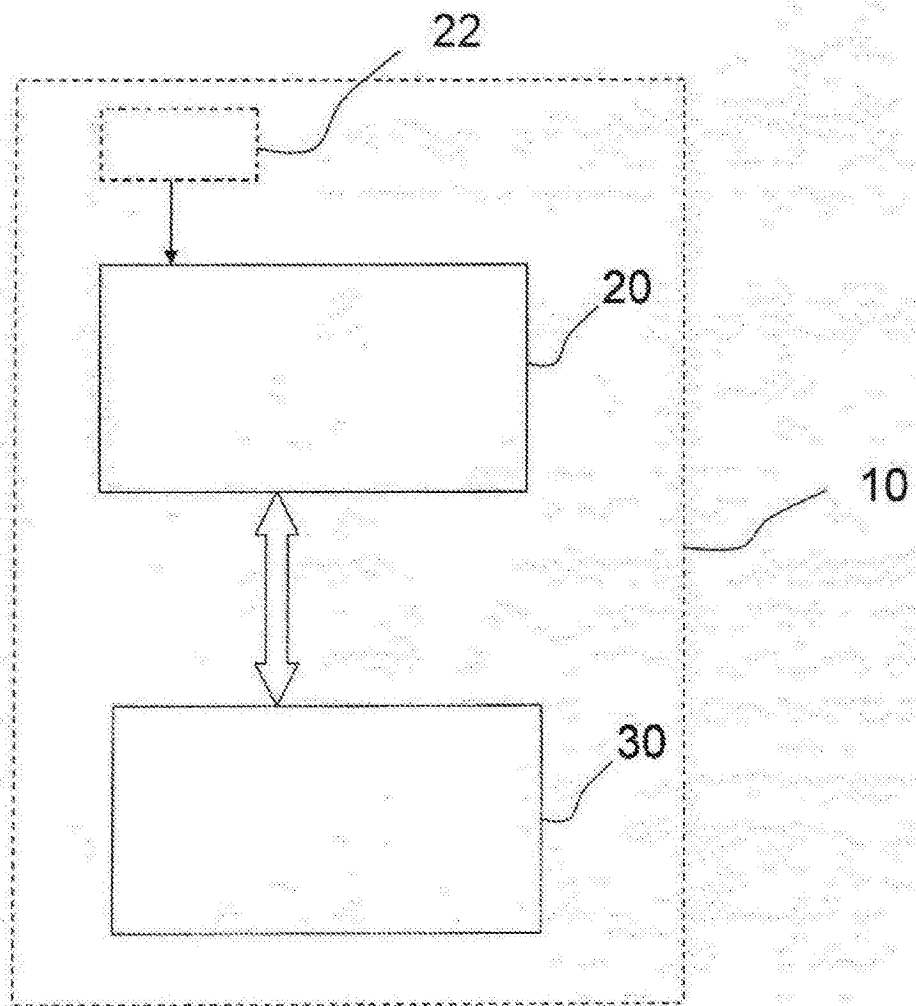


图1

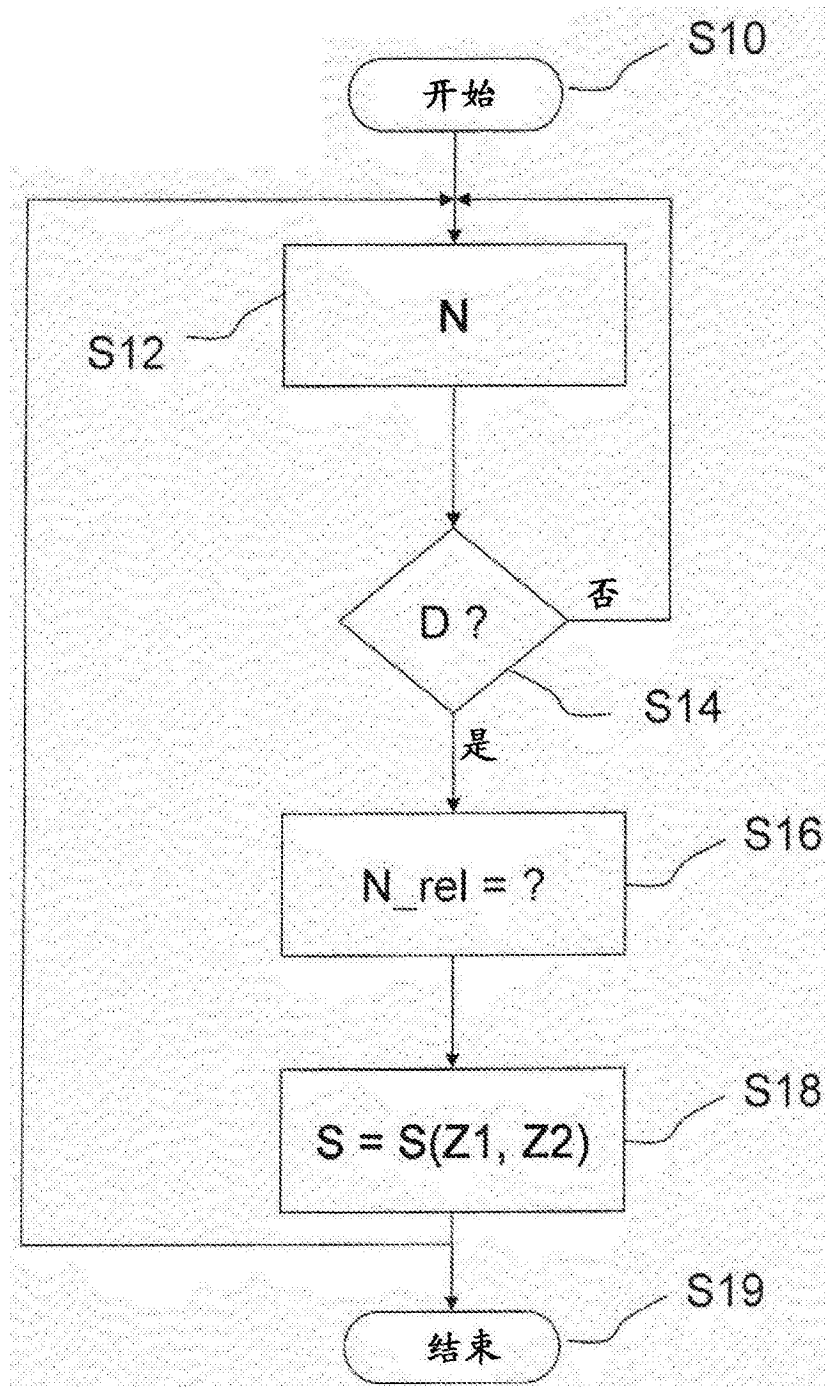


图2

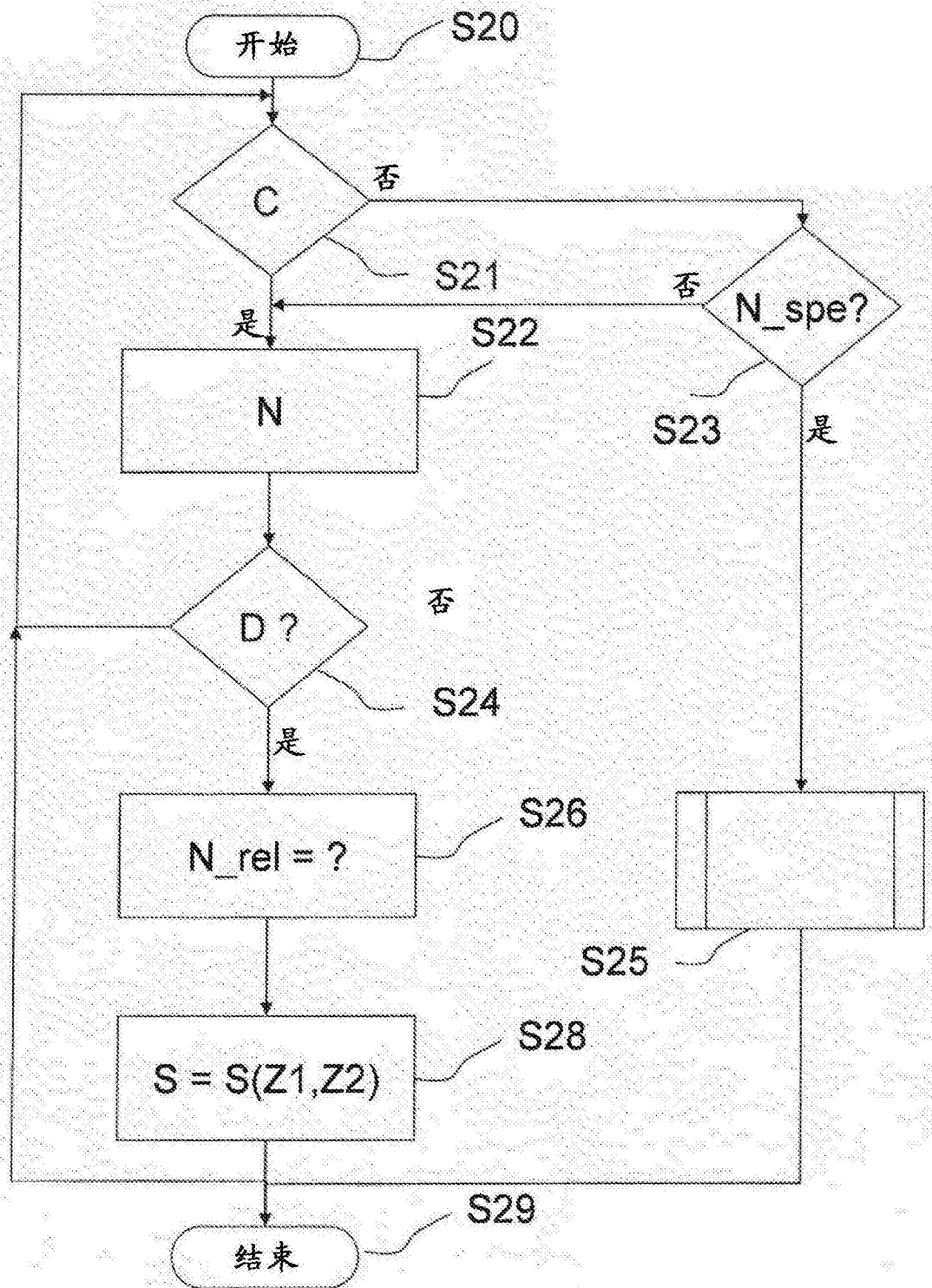


图3