



(12) 发明专利申请

(10) 申请公布号 CN 113169925 A

(43) 申请公布日 2021. 07. 23

(21) 申请号 201980083258.3	(74) 专利代理机构 中国专利代理(香港)有限公司 72001
(22) 申请日 2019.11.27	代理人 姬亚东 刘春元
(30) 优先权数据 102018221954.0 2018.12.17 DE	(51) Int.Cl. H04L 12/403 (2006.01) H04L 29/06 (2006.01) H04L 12/40 (2006.01) G06F 21/56 (2006.01) H04L 9/32 (2006.01)
(85) PCT国际申请进入国家阶段日 2021.06.16	
(86) PCT国际申请的申请数据 PCT/EP2019/082704 2019.11.27	
(87) PCT国际申请的公布数据 W02020/126365 DE 2020.06.25	
(71) 申请人 罗伯特·博世有限公司 地址 德国斯图加特	
(72) 发明人 C·波尔 F·施通普夫	

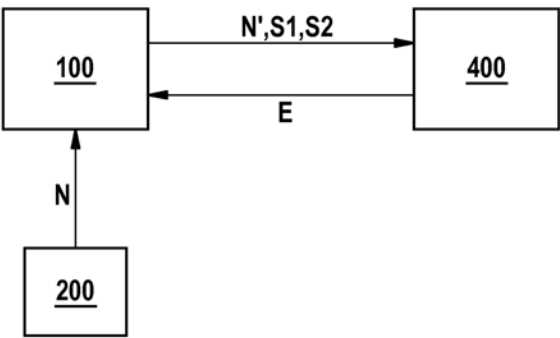
权利要求书2页 说明书6页 附图3页

(54) 发明名称

计算装置和用于运行计算装置的方法

(57) 摘要

计算装置,特别是用于机动车辆的控制设备的计算装置,其中所述计算装置被构造为从至少一个外部单元接收消息,其中所述计算装置被构造为至少暂时地存储接收到的消息并且将所述接收到的消息中的多个消息传送给密码模块,该密码模块被构造为对传送的消息进行检查。



1. 计算装置(100;100a),特别是用于机动车辆的控制设备(700)的计算装置,其中所述计算装置(100;100a)被构造为从至少一个外部单元(200)接收(300)消息(N),其中所述计算装置(100;100a)被构造为至少暂时地存储(302)接收到的消息(N)并且将所述接收到的消息(N)中的多个消息(N')传送(304)给密码模块(400;400'),所述密码模块被构造为对传送的消息(N')进行检查(502)。

2. 根据权利要求1所述的计算装置(100;100a),其中所述计算装置(100;100a)被构造为从所述密码模块(400;400')接收(306)所述检查(502)的结果(E)并且根据所述检查(502)的结果(E)处理(308)所述接收到的消息(N)中的多个消息(N')中的至少一个。

3. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中所述计算装置(100;100a)被构造为在将所述接收到的消息(N)中的多个消息(N')传送(312)给所述密码模块(400;400')之前等待(310)可预给定的最小数量的接收的消息。

4. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中所述计算装置(100;100a)被构造为在将特别是在可预给定的持续时间期间接收到的消息(N)中的多个消息(N')传送(322)给所述密码模块(400;400')之前,等待(320)所述可预给定的持续时间。

5. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中接收到的消息(N)的至少暂时存储(302)包括将所述接收到的消息(N)至少暂时存储(3020)在能够由所述计算装置(100;100a)和所述密码模块(400;400')两者访问的存储装置(104')中,并且其中所述传送(304;312;322)包括以下步骤:传递(3022)第一控制信息(S1),所述第一控制信息表征所述存储装置(104')的存储有所述接收到的消息(N)的存储区域。

6. 根据权利要求5所述的计算装置(100;100a),其中所述第一控制信息(S1)包括至少一个指针和/或接收到的消息(N)的数量。

7. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中所述计算装置(100;100a)被构造为将第二控制信息传递到所述密码模块(400;400'),其中所述第二控制信息表征所述存储装置(104')中的以下存储区域或地址,所述密码模块(400;400')应当将所述检查(502)的结果(E)或所述结果(E)写入所述存储区域或所述地址。

8. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中所述计算装置(100;100a)被构造为,如果接收到的消息还没有被所述密码模块(400;400')检查(502),则不对所述接收到的消息进行处理(308)。

9. 根据前述权利要求中的至少一项所述的计算装置(100;100a),其中所述密码模块(400;400')集成到所述计算装置(100;100a)中和/或所述密码模块(400;400')与所述计算装置(100;100a)布置在相同的半导体衬底(600)上。

10. 用于运行计算装置(100;100a)的方法,所述计算装置特别是用于机动车辆的控制设备(700),其中所述计算装置(100;100a)从至少一个外部单元(200)接收(300)消息(N),其中所述计算装置(100;100a)至少暂时存储(302)接收到的消息(N)并将所述接收到的消息(N)中的多个消息(N')传送(304)给密码模块(400;400'),所述密码模块被构造为对传送的消息(N')进行检查(502)。

11. 用于计算装置(100;100a),特别是用于根据权利要求1至9中至少一项所述的计算装置(100;100a)的密码模块(400;400'),其中所述密码模块(400;400')被构造为从所述计算装置(100;100a)接收(500)多个消息(N')并检查(502)接收到的消息。

12. 根据权利要求11所述的密码模块(400;400'),其中使用基于密钥的消息认证码CMAC(英语:Cipher-based Message Authentication Code)来执行所述检查(502)。

13. 根据权利要求11至12中的至少一项所述的密码模块(400;400'),其中所述密码模块(400;400')被构造为将所述检查(502)的结果(E)发送(504)到所述计算装置(100;100a),其中所述发送(504)特别是包括将表征所述结果(E)的结果信息写入存储装置(104')的可预给定存储区域中,所述计算装置(100;100a)和所述密码模块(400;400')都能够访问所述存储装置。

14. 根据权利要求1至9中至少一项所述的计算装置(100;100a)和/或根据权利要求10所述的方法和/或根据权利要求11至13中至少一项所述的密码模块(400;400')用于处理消息(N)的用途,所述消息特别是经由车辆、特别是机动车辆的总线系统传送的消息。

计算装置和用于运行计算装置的方法

技术领域

[0001] 本公开涉及一种计算装置,特别是用于机动车辆的控制设备的计算装置,其中所述计算装置被构造为从至少一个外部单元接收消息。

[0002] 本公开还涉及一种用于运行这种计算装置的方法。

发明内容

[0003] 优选的实施方式涉及一种计算装置,特别是用于机动车辆的控制设备的计算装置,其中所述计算装置被构造为从至少一个外部单元(例如其他控制设备)接收消息,其中所述计算装置被构造为至少暂时地存储接收到的消息并且将所述接收到的消息中的多个消息传送给密码模块,该密码模块被构造为对传送的消息进行检查。通过这种方式可以有效地检查传送的多个消息。

[0004] 在其他优选的实施方式中规定,所述计算装置被构造为从所述密码模块接收所述检查的结果,并且根据所述检查的结果处理所述接收到的消息中多个消息中的至少一个。

[0005] 在其他优选的实施方式中规定,所述计算装置被构造为在将所述接收到的消息中的多个消息传送给所述密码模块之前等待可预给定的最小数量的接收的消息。

[0006] 在其他优选的实施方式中规定,所述计算装置被构造为在将特别是在可预给定的持续时间期间接收到的消息中的多个消息传送给所述密码模块之前,等待所述可预给定的持续时间。

[0007] 在其他优选的实施方式中规定,接收到的消息的至少暂时存储包括将所述接收到的消息至少暂时存储在可由所述计算装置和所述密码模块两者访问的存储装置中,其中所述传送包括以下步骤:传递第一控制信息,所述第一控制信息表征所述存储装置的存储有所述接收到的消息的存储区域。

[0008] 在其他优选的实施方式中规定,所述第一控制信息包括至少一个指针和/或所接收到的消息的数量。

[0009] 在其他优选的实施方式中规定,所述计算装置被构造为将第二控制信息传递到所述密码模块,其中所述第二控制信息表征所述存储装置中的以下存储区域或地址,所述密码模块应当将所述检查的结果或所述结果写入所述存储区域或所述地址。

[0010] 在其他优选的实施方式中规定,所述计算装置被构造为,如果接收到的消息还没有被所述密码模块检查,则不对所述接收到的消息进行处理。由此确保仅处理由所述密码模块检查过的消息。

[0011] 在其他优选的实施方式中规定,所述密码模块集成到所述计算装置中和/或所述密码模块与所述计算装置布置在相同的半导体衬底上,这导致特别小构造的配置。

[0012] 在其他优选的实施方式中还可以规定,作为从外部单元接收的消息N的替代或补充,所述计算装置通常从另外的源获得或确定数据或消息(例如还由所述计算装置本身形成的数据或消息),并且可选地应用密码方法(特别是通过所述密码模块)来处理或可以处理所述数据或消息,例如配备或可以配备密码签名。为此,在其他优选的实施方式中,所述

计算装置可以将所提到的(从另外的源获得和/或自己形成的)消息传送给所述密码模块,优选地又是多个所提到的消息,其中在其他优选的实施方式中所述密码模块为这些消息配备密码签名(例如代替上述检查),优选地首先为所有所提到的多个消息配备签名,并且在其他优选的实施方式中,将配备有签名的消息然后传送到所述计算装置,然后在其他优选的实施方式中所述计算装置将经过签名的消息例如传送到其他计算装置或控制设备。

[0013] 其他优选的实施方式涉及一种用于运行计算装置的方法,所述计算装置特别是用于机动车辆的控制设备,其中所述计算装置从至少一个外部单元接收消息,其中所述计算装置至少暂时存储接收到的消息并将所述接收到的消息中的多个消息传送给密码模块,所述密码模块被构造为对传送的消息进行检查。

[0014] 其他优选的实施方式涉及一种用于计算装置,特别是用于根据实施方式的计算装置的密码模块,其中所述密码模块被构造为从所述计算装置接收多个消息并检查接收到的消息。

[0015] 在其他优选的实施方式中规定,使用基于密钥的消息认证码CMAC(英语:Cipher-based Message Authentication Code)来执行所述检查。由此实现了特别有效的检查。与CMAC方法的示例性设计有关的互联网出版物例如可在<https://doi.org/10.6028/2Fnist.sp.800-38b>中调用。

[0016] 在其他优选的实施方式中规定,所述密码模块被构造为将所述检查的结果发送到所述计算装置,其中该发送特别是包括将表征所述结果的结果信息写入存储装置的可预给定存储区域中,所述计算装置和所述密码模块都可以访问所述存储装置。

[0017] 其他优选的实施方式涉及根据实施方式的计算装置和/或根据实施方式的方法和/或根据实施方式的密码模块来处理消息、特别是经由车辆的总线系统传送的消息的用途,所述车辆特别是机动车辆。

附图说明

[0018] 本发明的其他特征、应用可能性和优点从以下对附图的各图中示出的本发明的实施例的描述中得出。在此,所描述或示出的所有特征单独地或以任何组合形成本发明的主题,而不管它们在权利要求或其引用中如何概括,以及不管它们在说明书或附图中如何表述或显示。

[0019] 在附图中:

图1示意性地示出了根据优选实施方式的计算装置的简化框图,

图2示意性地示出了根据其他优选实施方式的方法的简化流程图,

图3示意性地示出了根据其他优选实施方式的方法的简化流程图,

图4示意性地示出了根据其他优选实施方式的方法的简化流程图,

图5A、5B分别示意性地示出了根据其他优选实施方式的方法的简化流程图,

图6示意性地示出了根据其他优选实施方式的计算装置的简化框图,

图7示意性地示出了根据其他优选实施方式的计算装置的简化框图,

图8示意性地示出了根据其他优选实施方式的半导体衬底的简化框图,以及

图9示意性地示出了根据其他优选实施方式的控制设备的简化框图。

具体实施方式

[0020] 图1示意性地示出了根据优选实施方式的计算装置100的简化框图。计算装置100被构造为从至少一个外部单元200(例如,控制设备)接收消息N(或通常任何数据),至少暂时存储接收到的消息N并且将接收到的消息N中的多个消息N'传送给密码模块400,该密码模块被构造为对传送的消息N'进行检查。通过这种方式,可以有效地检查传送的多个消息N',并且可以通过计算装置100以特别节省资源的方式(例如作为连贯的数据块)将多个消息N'传送至密码模块400,例如与各个消息的重复传送相反。

[0021] 图2示意性地示出了根据其他优选实施方式的方法的简化流程图。在步骤300中,设备100(图1)从外部单元200(或从多个不同的单元,未示出)接收消息N(或通常任何数据)。在步骤302中,计算装置100至少暂时存储接收到的消息N。在步骤304中,计算装置100将接收到的消息中的多个消息N'传送给密码模块400以进行检验。

[0022] 在其他优选的实施方式中规定,计算装置100被构造为从密码模块400接收检查的结果E(图1),类似于图2中的可选步骤306,并且根据所述检查的结果E处理接收到的消息N中多个消息中的至少一个,类似于图2中的可选步骤308。

[0023] 在其他优选的实施方式中,计算装置100可以在步骤304中的传送之后并且特别是在根据步骤306接收结果E之前执行其他任务,由此密码模块400必要时检查之前确定的待检验消息所需要的时间段可以由计算装置100用于其他方面。例如,在所提及的时间段中可以由计算装置100处理早前由密码模块400传达的结果或所属的接收到的消息。

[0024] 图3示意性地示出了根据其他优选实施方式的方法的简化流程图,该流程图描述了密码模块400对消息的处理。在步骤500中,密码模块400接收在步骤304中已经从计算装置100传送到密码模块400的多个消息N'。在步骤502中,密码模块400检查从计算装置100接收的消息。在其他优选的实施方式中,使用基于密钥的消息认证码CMAC来执行根据图3的步骤502的检查。例如,可以为所涉及的待检查的消息设置CMAC参考值,密码模块400可以访问该CMAC参考值。对于检查步骤502,密码模块400可以有利地根据接收到的待检查的消息使用CMAC方法来形成当前CMAC值,并将该当前CMAC值与所述CMAC参考值进行比较。如果该比较得出相互比较的值相同,则密码模块400可以推断出被检查消息的真实性并提供对应的检查结果E。如果比较值彼此不一致,则可以推断出当前接收到的消息和被检查的消息不正常,例如已被操纵(和/或已被意外地篡改)。

[0025] 在其他优选的实施方式中,可以由计算装置100向密码模块400提供用于检查502的一个或多个参考值,特别是用于将由密码模块400检查的消息的一个或多个CMAC参考值。例如,计算装置100可以将所述参考值或CMAC参考值连同多个待检查的消息N'一起传送给密码模块400。

[0026] 在其他优选的实施方式中,为此例如可以使用以下数据格式。向待检查的消息(“纯文本”)分配索引值,该索引值使得该消息能够在多个待检查的消息N'中得到明确标识。可选地向待检查的消息分配(CMAC)参考值。进一步可选地,向待检查的消息分配密钥信息(“密钥ID”),该密钥信息表征与所述待检查的消息相关联的特殊密码密钥。因此在其他优选的实施方式中,具有上面示例性描述的数据格式的数据组可以包含以下元素中的至少一个:a)索引值,b)消息的内容(“纯文本”),c)(CMAC)参考值,d)密钥信息(“密钥ID”)。在其他优选的实施方式中,在传送步骤304(图2)中,除了待检查的消息之外,根据其他优选的实

施方式,还可以将具有示例性描述的数据格式的上述元素a)、c)、d)中的一个或多个传送到密码模块400,其中进而有利地将所提到的多个消息M'或对应的多个上述数据组传送到密码模块400,所述多个上述数据组与所提到的多个消息M'对应。

[0027] 在根据图3的步骤504中,密码模块400将检查502(图3)的结果E(图1)发送到计算装置100,其中计算装置100可以根据结果E以可选的步骤306和/或308继续前面已经参考图2描述的方法。

[0028] 在其他优选的实施方式中,通过多个消息N'从计算装置100向密码模块400的传送302(图2)得出其他优点,即密码模块400也可以一次性检查多个传送的消息,特别是在此过程中无需进一步与计算装置100通信(或中断多个消息N'的检查以与计算装置100通信),以例如重新加载待检查的各个其他消息。更确切地说,可以首先以所述方式在密码模块400内检查所提到的多个消息N',类似于根据图3的步骤502,并且在完全检查了所提到的多个消息N'之后才将结果E传达给计算装置100。

[0029] 在其他优选的实施方式中,类似于来自图4的简化流程图而规定,计算装置100被构造为在将所述接收到的消息中的多个消息N'(图1)传送给密码模块400之前,类似于步骤312,等待可预给定最小数量的接收到的消息,类似于步骤310。由此,接收到的多个消息可以有利地由计算装置100捆绑并且在一个传送过程中传送给密码模块400。

[0030] 在其他优选的实施方式中,类似于来自图5A的简化流程图而规定,计算装置100被构造为在将特别是在可预给定的持续时间内接收到的消息中的多个消息N'传送给密码模块400之前,类似于步骤322,等待所述可预给定的持续时间,类似于步骤320。由此,在从至少一个其他单元200到达计算装置100的多个消息N以多个消息N'的形式传输到密码模块400以进行检查之前,也可以有利地对所述多个消息N进行捆绑。

[0031] 在其他优选的实施方式中,类似于根据图5B的简化流程图而规定,通过计算装置100至少暂时存储接收到的消息包括在存储装置中至少暂时存储3020所述接收到的消息,计算装置100和密码模块都可以访问400所述存储装置,其中传送3022包括以下步骤:传递第一控制信息S1(图1),该第一控制信息S1表征所述存储装置的存储有所述接收到的消息的存储区域。例如,第一控制信息S1可以包含指向所述存储装置的对应存储区域的至少一个指针。

[0032] 在其他优选的实施方式中,除了传送待检查的多个消息M'之外,通过这种方式还可以附加地将分配给相应消息的元素a)索引值,c)(CMAC)参考值,d)密钥信息(“密钥ID”)中的一个或多个有效地传送到密码模块400。

[0033] 图6示意性地示出了根据其他优选实施方式的简化框图。例如,图1中的计算装置100可以具有根据图6的配置100a。配置100a具有至少一个计算单元102和分配给计算单元102的至少一个存储装置104,所述存储装置用于至少暂时存储计算机程序PRG,其中计算机程序PRG特别是被构造用于控制计算装置100的运行或配置100a,特别是用于执行根据实施方式的方法。

[0034] 在其他优选的实施方式中,计算单元102具有以下元件中的至少一个:微处理器、微控制器、数字信号处理器(DSP)、可编程逻辑模块(例如FPGA,即现场可编程门阵列)、ASIC(专用集成电路)、硬件电路。在其他优选的实施方式中,它们的组合也是可以想到的。

[0035] 在其他优选的实施方式中,存储装置104具有以下元件中的至少一个:易失性存储

器104a(特别是工作存储器(RAM)),非易失性存储器104b(特别是闪存EEPROM)。计算机程序PRG优选地存储在非易失性存储器104b中。

[0036] 在其他优选的实施方式中,还设置了上面已经描述的存储装置104',计算装置100、100a和密码模块400都可以访问该存储装置104'。如同样已经描述的,在其他优选的实施方式中,由计算装置100、100a接收的消息N可以至少暂时存储在存储装置104'中。在其他优选的实施方式中,可以为此定义至少一个接收缓冲器以用于待接收的消息。

[0037] 在其他优选的实施方式中,存储装置104'也可以形成存储装置104的一部分或集成到该存储装置104中。通过这种方式,消息N可以特别有效地从计算装置100传送到密码模块400。例如,在其他优选的实施方式中,将第一控制信息S1从计算装置100传输到密码模块400就可以足够了,以便密码模块400可以从存储装置104'中读取或加载待检查的消息。

[0038] 在其他优选的实施方式中规定,第一控制信息S1包括至少一个指针(例如指向存储装置104'的包括待检查的消息N的存储区域)和/或接收到的消息的数量。

[0039] 在其他优选的实施方式中规定,计算装置100、100a被构造为将第二控制信息S2(图1)传递到密码模块400,其中第二控制信息S2表征存储装置104中的以下存储区域或地址,密码模块400应当将检查502(图3)的结果或结果E(图1)写入该存储区域或该地址。

[0040] 在其他优选的实施方式中规定,计算装置100、100a被构造为,如果接收到的消息N还没有被密码模块400检查过,则不对所述接收到的消息N进行处理。由此确保了仅处理由密码模块400检查过的消息。

[0041] 在其他优选的实施方式中,类似于根据图7的简化框图而规定,密码模块400'集成到计算装置100a中。

[0042] 在其他优选的实施方式中,类似于根据图8的简化框图而规定,密码模块400与计算装置100布置在相同的半导体衬底600上,这导致特别小构造的配置。

[0043] 在其他优选的实施方式中规定,密码模块400、400'被构造为将检查502(图3)的结果E发送到计算装置100、100a,其中所述发送特别是包括将表征结果E的结果信息写入存储装置104'(图6)的可预给定存储区域中,计算装置100、100a和密码模块400、400'都可以访问该存储装置104'。在其他优选的实施方式中,可以向结果E的分配给多个消息M'中不同消息的不同结果值例如添加上面已经描述的索引值,以便能够实现相应的结果值向对应经过检查的消息的明确分配。

[0044] 其他优选的实施方式涉及根据实施方式的计算装置100、100a和/或根据实施方式的方法和/或根据实施方式的密码模块400、400'用于处理消息N(或通常任何数据)的用途,所述消息特别是经由车辆、特别是机动车辆的总线系统传递的消息。

[0045] 在其他优选的实施方式中,类似于根据图9的示意性框图,计算装置100是控制设备700的组成部分,所述控制设备特别是用于机动车辆,其中可选地,密码模块400同样可以形成控制设备700的一部分。

[0046] 在其他优选的实施方式中也可以规定,作为将从外部单元200接收的消息N的替代或补充,计算装置100通常从另外的源获得或确定数据或消息(例如也由计算装置100本身形成的数据或消息),并且可选地应用密码方法来处理所述数据或消息,例如配备密码签名。为此,在其他优选的实施方式中,类似于前面参照图2描述的过程,计算装置100可以将所提到的(例如自己形成的)消息传送给密码模块400,优选地又是多个所提到的消息,其中

密码模块400为这些消息配备密码签名以代替上面参考图3描述的检查502,优选地首先为所有所提到的多个消息配备签名,并且将配备有签名的消息然后传送到计算装置100,然后在其他优选的实施方式中所述计算装置将经过签名的消息例如传送到其他计算装置或控制设备。在其他优选的实施方式中,也可以为了产生或添加所述签名以及计算装置100和密码模块400之间的对应数据交换而使用上面参考图6描述的存储装置104',两个设备100、400都可以访问该存储装置104'。换言之,在其他优选的实施方式中可以规定,为了通过密码模块400产生签名还基于指针地与计算装置100进行对应的数据交换,在该数据交换中计算装置100与密码模块400交换对应的指针,所述指针指向共享存储装置104'的相应存储区域,其中这些存储区域包括例如要配备签名的消息和/或已配备有签名的消息。

[0047] 根据这些实施方式的原理使得可以通过计算装置100、100a特别有效地处理消息N。这既涉及在计算装置100、100a中从外部单元200接收的消息的处理,又涉及应当在计算装置100中形成或签名的消息的处理。多个消息N'到密码模块400的相应传输和/或由密码模块400对多个消息N'的处理决定了特别是计算装置100、100a的计算资源的节省并且避免了出现在传统系统中的通信开销,在传统系统中待检查的消息由所述计算装置单独处理或可以单独传送到密码模块400。

[0048] 此外,通过根据实施方式的原理的应用得到从计算装置100、100a到密码模块400的传输过程的最小化,特别是关于安全关键的信息的传输过程的最小化,由此进一步提高了安全性。

[0049] 在其他优选的实施方式中,如同等待的可预给定最小数量的接收的消息(类似于图4中的步骤310)和/或根据图5A中步骤320的可预给定持续时间,可以配置或参数化多个消息N'的值。由此根据实施方式的原理可以有效地适配不同的目标系统,例如控制设备,其中特别是可以考虑相应控制设备的通信负载(每个时间单位要处理的消息数量)和/或计算资源和/或存储资源。此外,根据实施方式的原理在计算装置100、100a对消息N的处理的可配置性方面提供了增加的灵活性。

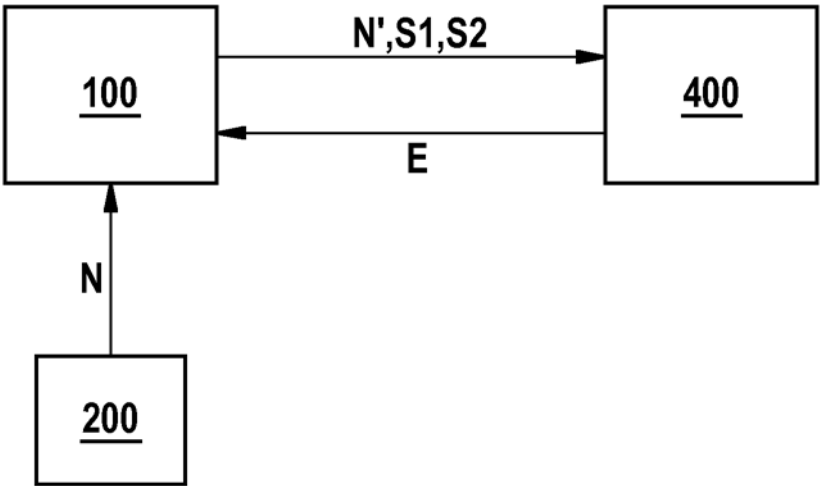


图 1

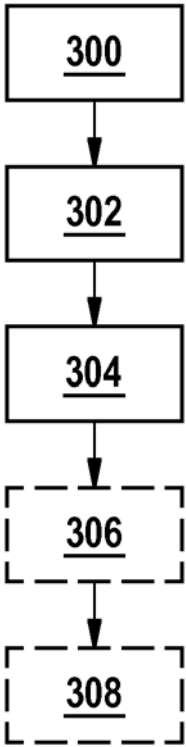


图 2

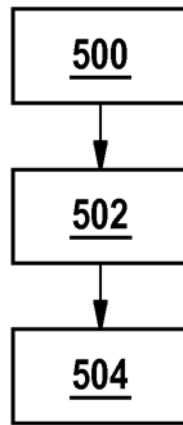


图 3

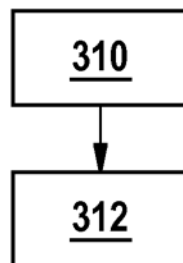


图 4

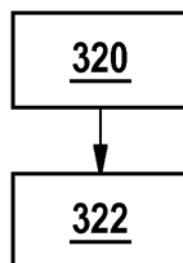


图 5a

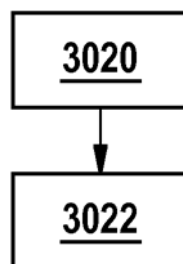


图 5b

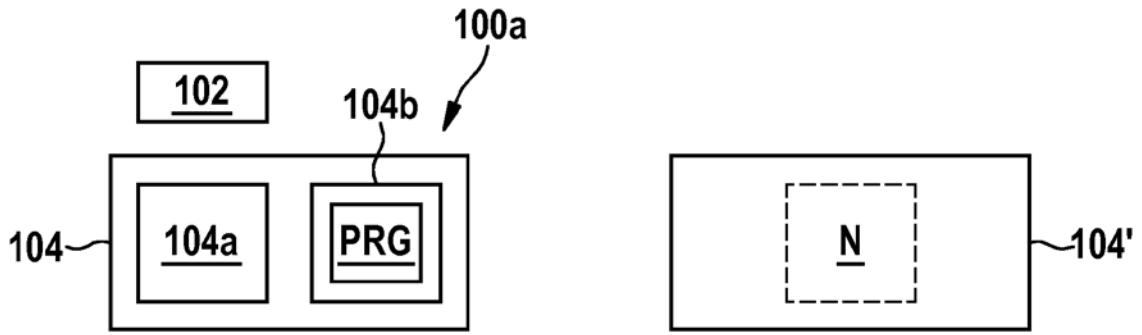


图 6



图 7

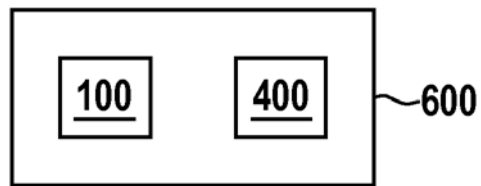


图 8



图 9