(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 103109280 A
(43)申请公布日 2013.05.15

(21)申请号 201180011794.6

(22)申请日 2011.02.07

(30)优先权数据
102010002472.4 2010.03.01 DE

(85)PCT申请进入国家阶段日
2012.08.31

(86)PCT申请的申请数据
PCT/EP2011/051714 2011.02.07

(87)PCT申请的公布数据
WO2011/107319 DE 2011.09.09

(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 M. 伊勒 O. 布贝克 J. 哈耶克
J. 索克罗拉希

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 杜荔南 卢江

(51)Int.Cl.
G06F 12/14(2006.01)
G06F 21/64(2013.01)
G06F 21/79(2013.01)
H04L 9/32(2006.01)

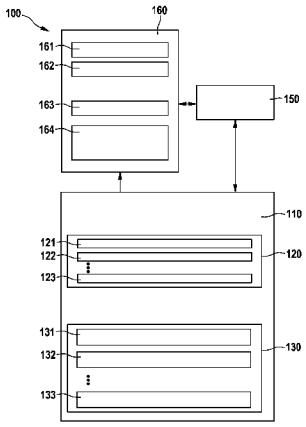
权利要求书1页 说明书3页 附图3页

(54)发明名称

用于验证非易失存储器的存储块的方法

(57)摘要

本发明涉及一种用于验证非易失存储器的存储块的方法，其中在使用秘密的密钥字的情况下在第一时刻确定(209)存储块(131,132,133)的第一认证代码并且存储(211)在认证代码存储表(120)中，在使用秘密的密钥字的情况下在用于验证的第二时刻确定(307)存储块(131,132,133)的第二认证代码并且与第一认证代码相比较(307)，以及当第一认证代码和第二认证代码一致时，所述存储块(131,132,133)得到验证(309)。



CN 103109280 A

1. 用于验证非易失存储器的存储块的方法，其中在使用秘密的密钥字的情况下在第一时刻确定（209）存储块（131,132,133）的第一认证代码并且存储（211）在认证代码存储表（120）中，在使用秘密的密钥字的情况下在用于验证的第二时刻确定（307）存储块（131,132,133）的第二认证代码并且与第一认证代码相比较（307），以及当第一认证代码和第二认证代码一致时，所述存储块（131,132,133）得到验证（309）。

2. 根据权利要求 1 所述的方法，其中将存储块（131,132,133）的存储地址和存储长度附加地存储（211）在认证代码存储表（120）中。

3. 根据权利要求 1 或 2 所述的方法，其中认证代码存储表（120）的存储地址和存储长度被存储（214）在地址存储块（162）中。

4. 根据权利要求 3 所述的方法，其中在使用秘密的密钥字的情况下确定认证代码存储表（120）的第三认证代码并且存储（214）在地址存储块（162）中。

5. 根据权利要求 3 或 4 所述的方法，其中将地址存储块设置在安全存储区（162）中。

6. 根据上述权利要求之一所述的方法，其中秘密的密钥字存储在安全的以及第三方无法读取的存储区（161）中。

7. 根据上述权利要求之一所述的方法，其中认证代码存储表（120）设置在非易失存储器（110）中。

8. 根据上述权利要求之一所述的方法，其中使用电子安全构件（160），该电子安全构件具有安全存储区（161,162）并且被设置为确定认证代码（121,122,123）。

9. 计算单元，其被设置为执行根据上述权利要求之一的方法。

用于验证非易失存储器的存储块的方法

技术领域

[0001] 本发明涉及一种用于验证非易失存储器的存储块的方法。

背景技术

[0002] 本发明可以用于识别对特定的存储块、尤其是非易失存储器(NVM，non volatile memory)的存储块的未经授权的操纵。本发明尤其适合于验证用于安全应用的计算单元(例如内嵌式系统)、控制设备等等的存储块。这种存储块例如包含用于实施与安全有关的或安全关键的功能的程序代码或者包含在非对称密码方法中使用的公共密钥，从而必须确保在存储块被分析或使用之前对这些存储块进行认证。

[0003] 已知使用哈希函数来验证这种存储块。在此，刚开始为每个待验证的存储块计算一个哈希值并且将该哈希值存储在专用的存储区中，该专用的存储区是防操纵的。在稍后的验证中，该存储块的哈希值被重新确定并且与所存储的值相比较。如果这两个值一致，则可以确定该存储块没有差错。这种技术例如在 TPM (Trusted Platform Module，受信平台模块)中采用。

[0004] 该已知方法的缺点在于，对于待验证的存储块的每个哈希值都必须提供防操纵的存储区。因此必须提供相对大的安全存储区，这是比较昂贵的。“安全存储区”应当被理解为不能被第三方写入的存储区。

[0005] 因此说明一种用于验证非易失存储器的存储块的节省资源的方法是值得期望的。

发明内容

[0006] 根据本发明，提出一种具有权利要求 1 的特征的方法。有利的设计是从属权利要求以及以下描述的主题。

[0007] 本发明采用以下措施，即为待验证的存储块确定认证代码，尤其是 MAC (Message Authentication Code，消息认证代码)。本发明在此使用秘密的密钥字或秘密的密钥，从而待提供的安全存储区的大小基本上限于可以容纳所述秘密的密钥字。秘密的密钥字被存储在安全存储区中，使得从外部不能接近该秘密的密钥字并且尤其是不能读取该秘密的密钥字。所述验证完全地和自动地在计算单元内进行。在现有技术中采用已知的哈希函数，从而原则上任何人都可以确定存储块的哈希值。因此哈希值必须被安全地存储，使得操纵被排除。但是在本发明中使用秘密的密钥字，从而与哈希值相当的所计算的认证代码恰好不能被任何人确定。因此特定的认证代码可以被存储在任何位置，尤其是还可以存储在不安全的存储区中。只是要将所使用的密钥字存储在安全存储区中。因此，显著减少了对安全存储空间的需求，这导致计算单元的简化以及成本节省。

[0008] 合适的是，在认证代码存储表中附加地存储待验证的存储块的存储地址和存储长度。由此可以容易地检查所存储的认证代码属于哪一个存储块。

[0009] 优选的，认证代码存储表的存储地址和存储长度被存储在地址存储块中，从而认证代码存储表总是与瞬时的情况匹配并且不存在灵活性限制，例如通过存储长度和固定预

先给定的存储地址。因此认证代码存储表尤其是还可以设置在非易失存储器中。

[0010] 在优选的设计中，在使用秘密的密钥字的情况下也确定认证代码存储表的认证代码并且存储在地址存储块中。由此在最大的防操纵性的情况下实现上述灵活性，因为总是可以检查实际上是否使用了正确的认证代码存储表。

[0011] 为了进一步提高安全性，合适的是将地址存储块设置在安全存储区中。“安全存储区”在此应当理解为第三方无法写入的存储区。

[0012] 在设计中，使用电子安全构件，其具有安全存储区并且被设置为确定认证代码。从而也可以通过简单的方式对已存在的系统进行加装。

[0013] 本发明的计算单元，例如汽车的控制设备尤其是可用程序技术设置为执行本发明的方法。该计算单元尤其是具有上述电子安全构件。

[0014] 以软件的形式来实施该方法也是有利的，因为这产生特别小的成本，尤其是当实施的控制设备还用于其它任务并且因此无论如何都存在时。用于提供计算机程序的合适的数据载体尤其是光盘、硬盘、闪存、EEPROM、CD-ROM、DVD 等。通过计算机网络（互联网，内部网，等）下载程序也是可行的。

[0015] 本发明的其它优点和设计由说明书和附图得到。

[0016] 应当理解，上述和下面还要阐述的特征不仅能以分别说明的组合，而且还能以其它组合或单独地使用，而不会脱离本发明的范围。

附图说明

[0017] 本发明借助附图中的实施例示意性示出并且将在下面参照附图详细描述。

[0018] 图 1 示出本发明计算单元的一种实施方式的框图。

[0019] 图 2 示出本发明方法的一种实施方式的在第一时刻进行的部分的流程图。

[0020] 图 3 示出本发明方法的一种实施方式的在第二时刻进行的部分的流程图。

具体实施方式

[0021] 在图 1 中以框图示意性示出本发明计算单元的优选实施方式，并且总体上用 100 表示。计算单元 100 除其它未示出的部件如 CPU、RAM 等之外包括三个部件 110, 150 和 160，它们有贡献于在所示出的优选实施方式中实现本发明并在下面按顺序解释。

[0022] 计算单元 100 具有非易失存储器（NVM）110，其中存储待验证的存储块 131, 132 等。在此例如可以涉及固件的组成部分，涉及密钥等等，从而应当保证存储块得到认证。在非易失存储器 110 中，存放具有各个表区域 121, 122 等的认证代码存储表 120。

[0023] 计算单元 100 还包括写入模块 150，该写入模块能够对非易失存储器 110 进行写入。写入模块 150 可以是 CPU 的一部分或外部部分。此外，计算单元 100 包括负责执行加密操作并且提供安全存储区的电子安全构件 160。安全构件 160 包括安全的、第三方无法读取的存储区 161，在该存储区 161 中存储用于产生认证代码的秘密的密钥字。此外，安全构件 160 包括用于容纳地址存储块的安全存储区 162，在该地址存储块中存放认证代码存储表 120 的认证代码、存储地址和存储长度。安全构件 160 还包括处理模块 163 以及可选地包括用于加速对称加密的协处理器 164。

[0024] 图 2 中描述了本发明方法的一种实施方式的在第一时刻执行的部分，该部分用于

产生认证代码。

[0025] 首先写入模块 150 在步骤 201 中在使用任意认证方法的情况下向安全构件 160 确认，使得写入模块 150 被授权对非易失存储器 110 进行写入。

[0026] 在步骤 202 中，安全构件 160 检查认证是否成功。如果认证不成功，则安全构件 160 在步骤 203 中将相应的通知发送给写入模块 150 并且在步骤 204 中中断该方法。

[0027] 相反如果认证成功，则安全构件 160 在步骤 205 中将相应的成功通知发送给写入模块 150。

[0028] 接着写入模块 150 在步骤 206 中以待保护的第一块，即根据图 1 的 131 开始，并且在步骤 207 中检查是否已经达到要保护的最后一块。如果不是，则写入模块 150 将所涉及块的存储地址和存储长度在步骤 208 中传送给安全构件 160。

[0029] 在步骤 209 中，安全构件 160 从非易失存储器 110 中读取所涉及的存储块并且借助存储在安全存储区 161 中的密钥字计算出所属的认证代码。该认证代码在步骤 210 中被传输给写入模块 150，该写入模块 150 在步骤 211 中将所述认证代码与块 131 的存储地址和存储长度一起写入到认证代码存储表 120 中，在此写入到表区域 121 中。

[0030] 在接下来的方法步骤 212 中，选择下一个块并且返回到步骤 207。如果在步骤 207 中相应频繁地执行了该方法之后确定最后一个块 n 已被处理，则在步骤 213 中将认证代码存储表 120 的存储地址和存储长度传送给安全构件 160，该安全构件 160 接着在步骤 214 中计算认证代码存储表 120 的认证代码并且将该认证代码与存储地址和存储长度一起存储在安全存储区 162 中。

[0031] 在运行期间执行的对存储块 131 等的验证在下面借助图 3 阐述。

[0032] 在步骤 301 中，写入模块 150 请求安全构件 160 验证认证代码存储表 120。

[0033] 接着安全构件 160 在步骤 302 中计算认证代码存储表 120 的认证代码，安全构件 160 可以从存储区 162 中读取该认证代码的位置和长度，并且将所计算的值与同样存储在存储区 162 中的值进行比较。安全构件 160 将该比较结果在方法步骤 303 中提供给写入模块 150，该写入模块 150 在步骤 304 中对结果进行分析。如果认证代码不一致，则将该结果传送给实例 309，该实例 309 基于该比较结果作出决定。

[0034] 但是如果认证代码一致，则写入模块 150 在步骤 305 中从认证代码存储表 120 读取待验证存储块的存储地址、存储长度和认证代码。例如，写入模块 150 在块 132 要被验证时读取表区域 122。

[0035] 在步骤 306 中，写入模块 150 将该数据传送给安全构件 160，该安全构件 160 在步骤 307 中借助所述数据读取在非易失存储器 110 中所涉及的存储块，例如 132，并且计算该存储块的认证代码。接着，安全构件 160 将新计算的认证代码与由写入模块 150 传送的认证代码进行比较，并且将比较结果在步骤 308 中传送给写入模块 150。

[0036] 写入模块 15 然后在步骤 309 中基于该比较结果产生相应的决定。

[0037] 利用本发明可以验证存储块并且将为此所需的对安全存储器的需要保持得小。

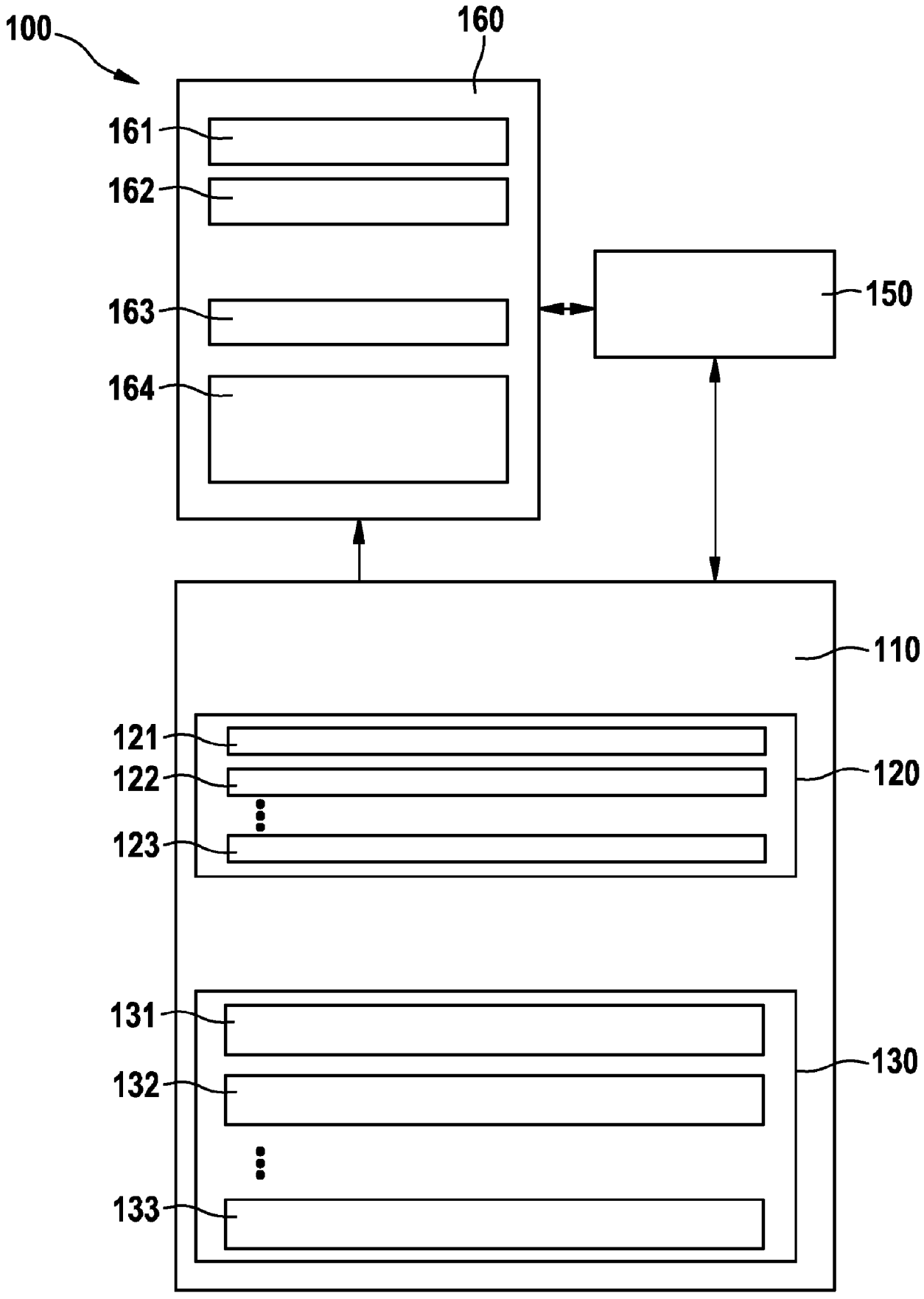


图 1

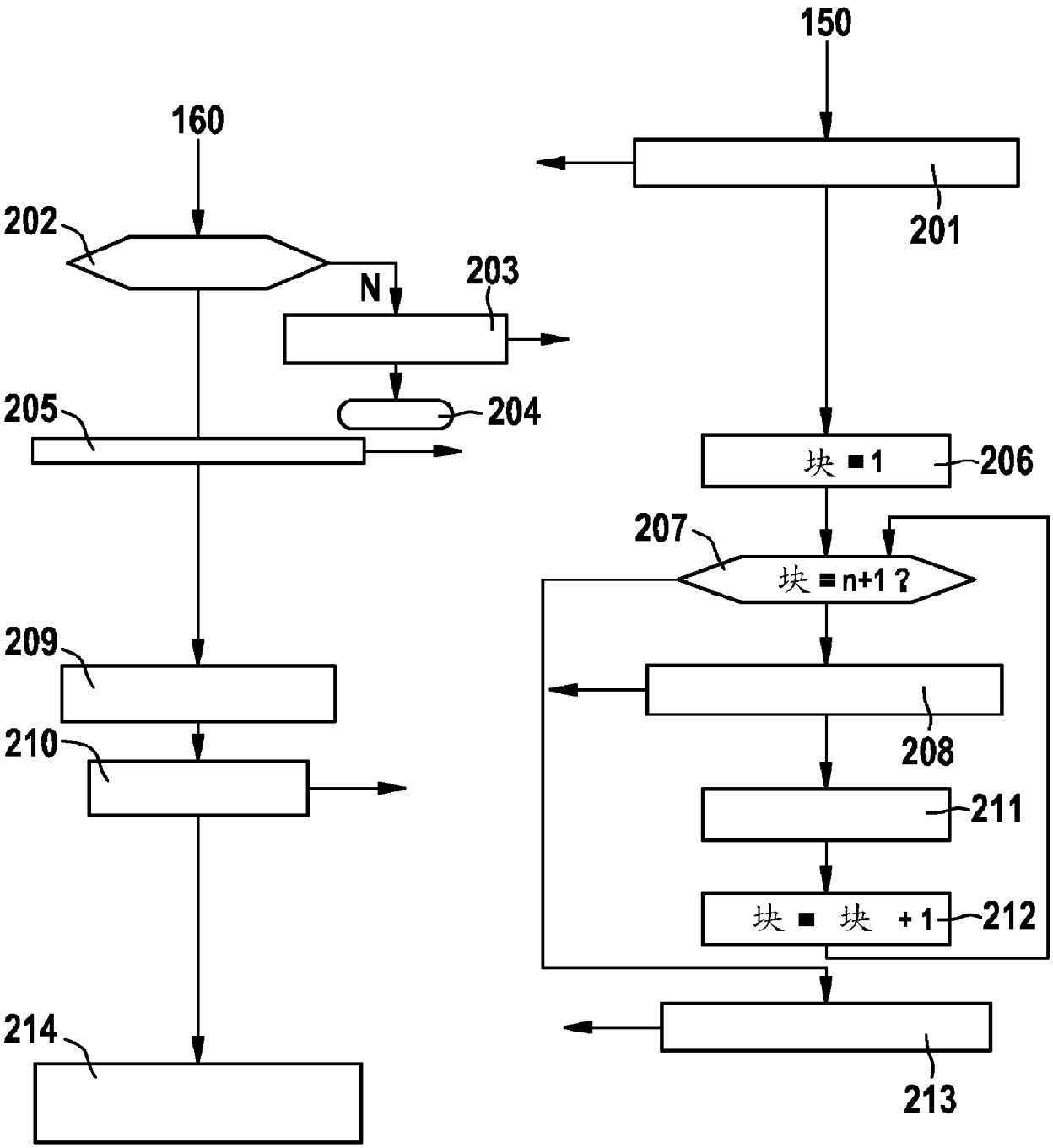

150
201
160
202
N
203
204
205
块 = 1
206
207
块 = n+1 ?
209
208
210
211
块 = 块 + 1
212
214
213

图 2

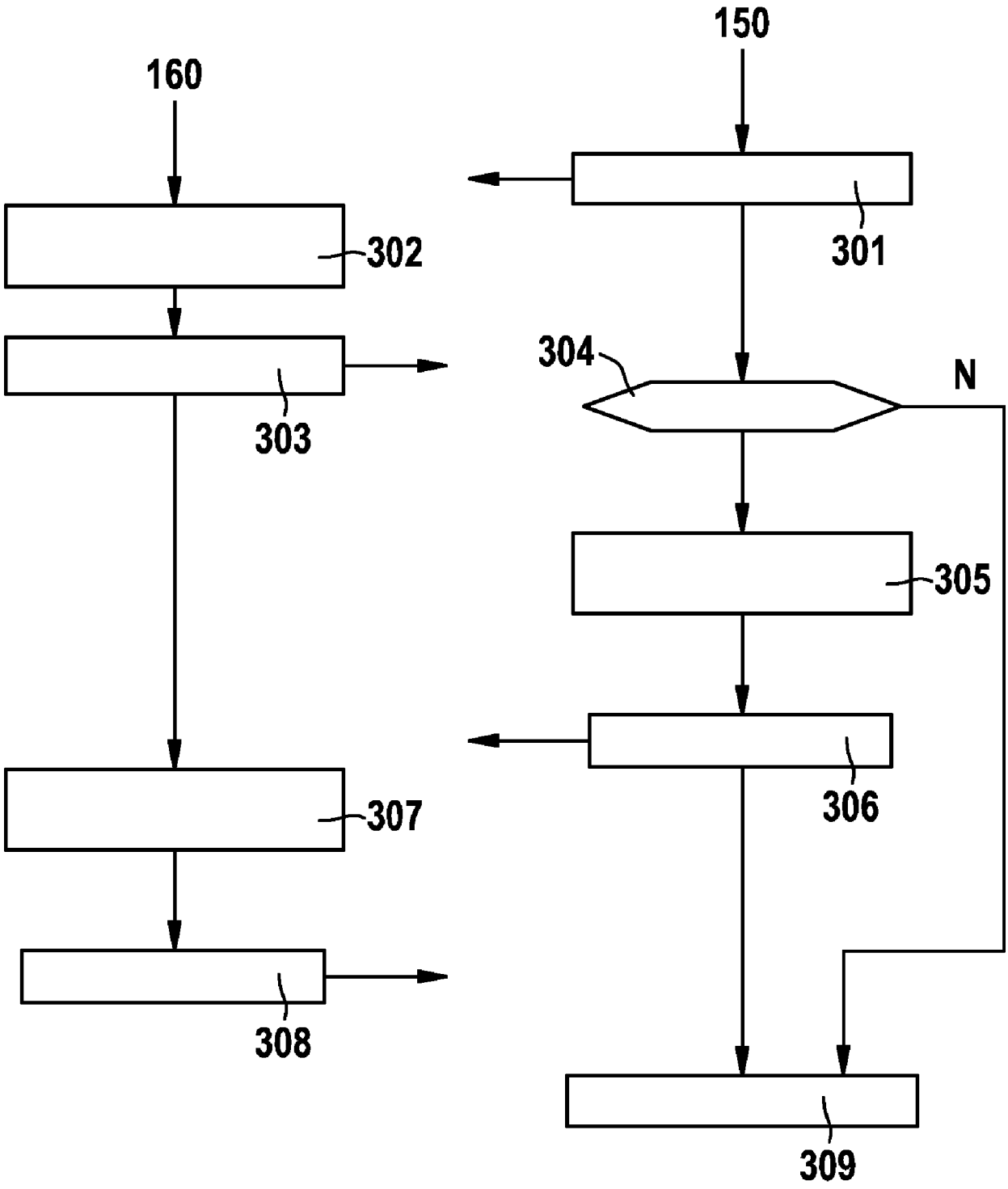


图 3