



(12) 发明专利

(10) 授权公告号 CN 118051919 B

(45) 授权公告日 2024. 08. 06

(21) 申请号 202410453827.1

(22) 申请日 2024.04.16

(65) 同一申请的已公布的文献号
申请公布号 CN 118051919 A

(43) 申请公布日 2024.05.17

(73) 专利权人 苏州萨沙迈半导体有限公司
地址 215000 江苏省苏州市姑苏区锦堂街8号6F

专利权人 合肥智芯半导体有限公司
上海萨沙迈半导体有限公司
天津智芯半导体科技有限公司

(72) 发明人 程雯 张恩勤

(74) 专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
专利代理师 张培培

(51) Int. Cl.

G06F 21/57 (2013.01)

G06F 9/4401 (2018.01)

(56) 对比文件

CN 114500064 A, 2022.05.13

CN 117610083 A, 2024.02.27

审查员 高莘尧

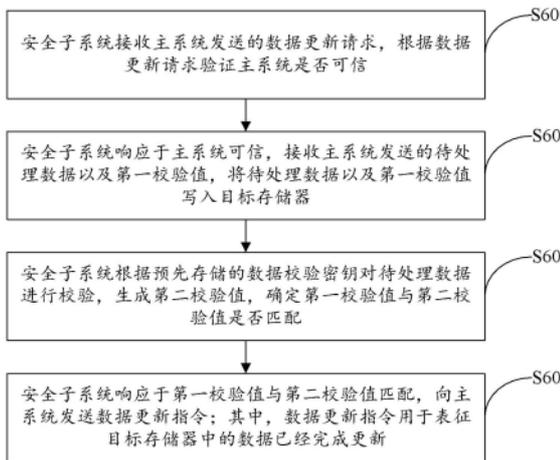
权利要求书2页 说明书13页 附图9页

(54) 发明名称

数据处理方法、芯片、电子设备以及存储介质

(57) 摘要

本发明提供一种数据处理方法、芯片、电子设备以及存储介质,所述方法包括:安全子系统接收主系统发送的数据更新请求,根据数据更新请求验证主系统是否可信;安全子系统响应于主系统可信,接收主系统发送的待处理数据以及第一校验值,将待处理数据以及第一校验值写入目标存储器;安全子系统根据预先存储的数据校验密钥对待处理数据进行校验,生成第二校验值,确定第一校验值与第二校验值是否匹配;安全子系统响应于第一校验值与第二校验值匹配,向主系统发送数据更新指令;其中,数据更新指令用于表征目标存储器中的数据已经完成更新。



1. 一种数据处理方法,其特征在于,应用于芯片,所述芯片包括安全子系统、主系统和目标存储器,所述安全子系统与所述目标存储器进行读写访问,所述主系统与所述目标存储器进行读访问;

所述方法包括:

所述安全子系统接收所述主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信;

所述安全子系统响应于所述主系统可信,向所述主系统发送可信认证结果,以使所述主系统根据所述可信认证结果获取待处理数据以及第一校验值;

所述安全子系统接收所述主系统发送的待处理数据以及第一校验值,将所述目标存储器中的数据的数据状态标记为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限;将所述待处理数据以及所述第一校验值写入所述目标存储器;

所述安全子系统根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配;

所述安全子系统响应于所述第一校验值与所述第二校验值匹配,将所述目标存储器中的数据的数据状态标记为有效状态;其中,所述有效状态用于表征所述目标存储器中的数据允许被执行;向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新;

所述主系统响应于确定所述芯片的启动信息,则读取所述目标存储器中的数据的数据状态;

所述主系统响应于所述目标存储器中的数据状态为有效状态,读取并执行所述目标存储器中的数据。

2. 根据权利要求1所述的数据处理方法,其特征在于,所述方法还包括:

所述安全子系统响应于所述主系统不可信,终止将所述待处理数据以及所述第一校验值写入目标存储器的流程。

3. 根据权利要求1所述的数据处理方法,其特征在于,所述方法还包括:

所述安全子系统响应于所述第一校验值与所述第二校验值不匹配,则将所述目标存储器中的数据的数据状态维持为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限。

4. 根据权利要求1所述的数据处理方法,其特征在于,所述方法还包括:

所述主系统响应于所述目标存储器中的数据状态为无效状态,禁止执行所述目标存储器中的数据,或,执行所述目标存储器中的部分数据。

5. 一种芯片,其特征在于,所述芯片包括安全子系统、主系统和目标存储器,所述安全子系统与所述目标存储器进行读写访问,所述主系统与所述目标存储器进行读访问;

所述安全子系统,被配置为:

接收所述主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信;

响应于所述主系统可信,向所述主系统发送可信认证结果,以使所述主系统根据所述可信认证结果获取待处理数据以及第一校验值;

所述安全子系统接收所述主系统发送的待处理数据以及第一校验值,将所述目标存储器中的数据的数据状态标记为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限;将所述待处理数据以及所述第一校验值写入所述目标存储器;

根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配;

响应于所述第一校验值与所述第二校验值匹配,将所述目标存储器中的数据的数据状态标记为有效状态;其中,所述有效状态用于表征所述目标存储器中的数据允许被执行;向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新;

所述主系统被配置为响应于确定所述芯片的启动信息,则读取所述目标存储器中的数据的数据状态;

所述主系统被配置为响应于所述目标存储器中的数据状态为有效状态,读取并执行所述目标存储器中的数据。

6. 一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1至4任意一项所述的方法。

7. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储计算机指令,所述计算机指令用于使所述计算机执行权利要求1至4任一所述方法。

数据处理方法、芯片、电子设备以及存储介质

技术领域

[0001] 本发明涉及数据处理技术领域,尤其涉及一种数据处理方法、芯片、电子设备以及存储介质。

背景技术

[0002] 随着信息安全技术的发展,针对嵌入式系统进行安全防护已经成为一种必需采取的措施。在嵌入式系统的安全防护中,需要确保执行的代码不被篡改,保证执行的代码都是可信的。

[0003] 现有技术中,一般的系统会在启动时通过MAC或者签名等方式验证代码的完整性和正确性,但是在验证过程中存在一些局限性,首先,每次启动时都需要进行代码验证,这会增加系统的启动时间。对于代码量较大的系统来说,这种影响尤为明显,可能导致启动过程变得缓慢,影响用户体验。其次,如果系统需要频繁地更新代码,那么每次更新后都需要重新进行验证,这也会增加系统的维护成本和时间开销。此外,如果攻击者能够找到方法绕过验证机制,或者在验证过程中进行干扰,那么系统的安全性就会受到威胁。

发明内容

[0004] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。为此,本发明的第一个目的在于提出一种数据处理方法,通过安全子系统对主系统的数据更新请求进行验证,以确保主系统是可信的,增强了系统的安全性,防止了恶意或未经授权的更新,进一步地,由持有可信密钥的安全子系统写入并校验待处理数据,确保数据在写入过程中没有被篡改,保证了数据的完整性,使得每次更新都是可靠和准确的。通过安全子系统与主系统的协同工作,确保整个数据更新流程更加有序和可靠,主核无需在每次启动时都对数据进行校验,节约了数据更新时间,且减少因数据不一致或错误更新而导致的系统故障,增强了系统的稳定性和可靠性。

[0005] 本发明的第二个目的在于提出一种芯片。

[0006] 本发明的第三个目的在于提出一种电子设备。

[0007] 本发明的第四个目的在于提出一种计算机可读存储介质。

[0008] 为达到上述目的,本发明第一方面实施例提出了一种数据处理方法,应用于芯片,所述芯片包括安全子系统、主系统和目标存储器,所述安全子系统与所述目标存储器进行读写访问,所述主系统与所述目标存储器进行读访问;其所述方法包括:所述安全子系统接收所述主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信;所述安全子系统响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入所述目标存储器;所述安全子系统根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配;所述安全子系统响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器

中的数据已经完成更新。

[0009] 另外,根据本发明上述实施例的数据处理方法还可以具有如下的附加技术特征:

[0010] 根据本发明的一些实施例,所述安全子系统响应于所述主系统可信之后,所述方法还包括:

[0011] 所述安全子系统向所述主系统发送可信认证结果,以使所述主系统根据所述可信认证结果获取所述待处理数据以及所述第一校验值。

[0012] 根据本发明的一些实施例,所述方法还包括:

[0013] 所述安全子系统响应于所述主系统不可信,终止将所述待处理数据以及所述第一校验值写入目标存储器的流程。

[0014] 根据本发明的一些实施例,所述安全子系统将所述待处理数据以及所述第一校验值写入目标存储器之前,所述方法还包括:

[0015] 所述安全子系统将所述目标存储器中的数据的数据状态标记为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0016] 根据本发明的一些实施例,所述安全子系统响应于所述第一校验值与所述第二校验值匹配之后,所述方法还包括:

[0017] 所述安全子系统将所述目标存储器中的数据的数据状态标记为有效状态;其中,所述有效状态用于表征所述目标存储器中的数据允许被执行。

[0018] 根据本发明的一些实施例,所述方法还包括:

[0019] 所述安全子系统响应于所述第一校验值与所述第二校验值不匹配,则将所述目标存储器中的数据的数据状态维持为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0020] 根据本发明的一些实施例,所述方法还包括:

[0021] 所述主系统响应于确定所述芯片的启动信息,则读取所述目标存储器中的数据的数据状态;

[0022] 所述主系统响应于所述目标存储器中的数据状态为有效状态,读取并执行所述目标存储器中的数据。

[0023] 根据本发明的一些实施例,所述方法还包括:

[0024] 所述主系统响应于所述目标存储器中的数据状态为无效状态,禁止执行所述目标存储器中的数据,或,执行所述目标存储器中的部分数据。

[0025] 根据本发明实施例的数据处理方法,通过安全子系统负责数据的更新和校验,并且在更新时及时更新代码是否有效的标志,芯片在启动时只需读取该标志,而无需对整个代码进行校验。这大大减少了启动时间,提高了系统的实时性,特别是在代码量大的系统上,这种优化效果更加明显。如果检测到数据被篡改或校验失败,安全子系统能够立即采取相应措施,如禁止主系统启动或限制其功能,从而及时阻止非法操作。这种实时防护机制提高了系统的安全性,并能够在发生安全问题时迅速做出响应。

[0026] 为达到上述目的,本发明第二方面实施例提出了一种芯片,所述芯片包括安全子系统、主系统和目标存储器,所述安全子系统与所述目标存储器进行读写访问,所述主系统与所述目标存储器进行读访问。

[0027] 所述安全子系统,被配置为:

[0028] 接收所述主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信;

[0029] 响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入所述目标存储器;

[0030] 根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配;

[0031] 响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新。

[0032] 根据本发明实施例提供的一种芯片,安全子系统用于接收主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信,响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入目标存储器,根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配,响应模块用于响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新。由此,该芯片通过安全子系统负责数据的更新和校验,并且在更新时及时更新代码是否有效的标志,芯片在启动时只需读取该标志,而无需对整个代码进行校验。这大大减少了启动时间,提高了系统的实时性,特别是在代码量大的系统上,这种优化效果更加明显。如果检测到数据被篡改或校验失败,安全子系统能够立即采取相应措施,如禁止主系统启动或限制其功能,从而及时阻止非法操作。这种实时防护机制提高了芯片的安全性,并能够在发生安全问题时迅速做出响应。

[0033] 为达到上述目的,本发明第三方面实施例提出了一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如上述所述的数据处理方法。

[0034] 为达到上述目的,本发明第四方面实施例提出的一种计算机可读存储介质,所述计算机可读存储介质存储计算机指令,所述计算机指令用于使所述计算机执行上述所述数据处理方法。

[0035] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0036] 为了更清楚地说明本发明或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0037] 图1为现有技术中的芯片结构示意图。

[0038] 图2为现有技术中的芯片代码更新流程示意图。

[0039] 图3为现有技术中的芯片安全启动流程示意图。

[0040] 图4为本发明实施例提供的芯片结构示意图。

[0041] 图5为本发明实施例提供的非易失性存储器示意图。

[0042] 图6为本发明实施例提供的应用于芯片的安全子系统的数据处理方法流程示意图。

[0043] 图7为本发明实施例提供的应用于芯片的主系统的数据处理方法流程示意图。

[0044] 图8为本发明实施例提供的数据处理方法应用于安全子系统以及主系统的交互流程示意图。

[0045] 图9为本发明实施例提供的芯片代码更新流程示意图。

[0046] 图10为本发明实施例提供的一种芯片示意图。

[0047] 图11为本发明实施例提供的一种更为具体的电子设备硬件结构示意图。

[0048] 附图标记:现有技术中的芯片结构100、主核101、安全子系统102、非易失性存储器103、邮箱模块104、本发明实施例提供的芯片结构400、安全子系统401、主系统402、目标存储器403、通信模块404、目标存储器控制器4031、目标存储器主阵列4032、总线主设备权限控制器4033、安全子系统1001、主系统1002、目标存储器1003、处理器1110、存储器1120、输入/输出接口1130、通信接口1140、总线1150。

具体实施方式

[0049] 为使本发明的目的、技术方案和优点更加清楚明白,以下结合具体实施例,并参照附图,对本发明进一步详细说明。

[0050] 需要说明的是,除非另外定义,本发明使用的技术术语或者科学术语应当为本发明所属领域内具有一般技能的人士所理解的通常意义。本发明中使用的“第一”、“第二”以及类似的词语并不表示任何顺序、数量或者重要性,而只是用来区分不同的组成部分。“包括”或者“包含”等类似的词语意指出现该词前面的元件或者物件涵盖出现在该词后面列举的元件或者物件及其等同,而不排除其他元件或者物件。“连接”或者“相连”等类似的词语并非限定于物理的或者机械的连接,而是可以包括电性的连接,不管是直接的还是间接的。“上”、“下”、“左”、“右”等仅用于表示相对位置关系,当被描述对象的绝对位置改变后,则该相对位置关系也可能相应地改变。

[0051] 如背景技术部分所述,随着嵌入式系统的广泛应用,其安全性问题日益凸显,特别是在对实时性要求较高的场景中,如何保证系统执行代码的完整性和正确性,同时减少启动时间,成为了一个亟待解决的技术难题。

[0052] 申请人在实现本发明的过程中发现,传统的嵌入式系统在上电启动时,通常通过MAC或签名等方式验证代码的完整性和正确性。然而,这种验证过程会增加系统的启动时间,尤其对于执行固件较大的系统,启动时间的延长更为明显。对于需要快速响应的实时性系统,过长的启动时间显然无法满足其性能要求。此外,现有技术对于代码篡改的防护存在局限性。一旦代码在运行时被篡改,现有技术往往无法及时发现,只能在下次启动时才能检测到,这无疑增加了系统面临的安全风险。如果系统在此期间执行了非法操作,可能会导致严重的后果。因此,如何在保证嵌入式系统代码安全性的同时,减少启动时间,提高对代码篡改的实时防护能力,成为了当前嵌入式系统安全领域亟待解决的技术问题。

[0053] 以下,通过具体的实施例进一步详细说明本发明的技术方案。

[0054] 参考图1,为现有技术中的芯片结构示意图。

[0055] 图1为现有技术中的芯片结构100,包括:主核101,安全子系统102,非易失性存储

器103 以及邮箱模块104。

[0056] 其中,非易失性存储器103(英语:non-volatile memory,缩写为NVM)是指当电流关掉后,所存储的数据不会消失的存储器。邮箱模块104即基于邮箱机制的收发消息的模块,将需要传递的消息内容指定接收方,可以将待处理数据传递到指定的系统端,用于辅助主核101和安全子系统102之间建立通信。

[0057] 其中,主核101与安全子系统102之间通过邮箱模块104通信连接,主核101与邮箱模块104之间可以进行读写访问,安全子系统102与邮箱模块104之间也可以进行读写访问。主核101与非易失性存储器103之间通信连接,主核101可以与非易失性存储器103之间进行读写访问,而安全子系统102与非易失性存储器103之间仅可以进行读访问。

[0058] 需要说明的是,安全子系统是整个芯片的可信根,密钥等重要安全数据全部存储在安全子系统内部。外界无法访问安全子系统内部的信息,也无法篡改其内部存储的内容,因此安全子系统被认为是安全的。而主核的安全等级会比安全子系统低,其非易失性存储器中存储的内容可以被主核随意修改。

[0059] 参考图2,为现有技术中的芯片代码更新流程示意图。

[0060] 现有技术中,主核开启更新流程,将待处理数据以及代码的可信校验值写入非易失性存储器中,其中,待处理数据可以理解为待更新的代码,可信校验值是主核预先从可信端获取到的初始校验值,可信端是安全子系统认证为可信的端。进一步地,主核通知安全子系统校验写入的代码,安全子系统接收到通知后,读取待处理数据,根据预先存储的密钥对待处理数据进行校验,生成新的校验值,将新生成的校验值与可信校验值相匹配,安全子系统向主核通知校验结果,若匹配,则表示针对待处理数据的校验结果正确,主核对代码的更新成功,结束更新;若不匹配,则表示针对待处理数据的校验结果错误,主核对代码的更新失败,结束更新。

[0061] 参考图3,为现有技术中的芯片安全启动流程示意图。

[0062] 为了防止主核执行的代码被篡改,会在安全启动时通过安全子系统来对主系统待执行的代码进行校验,校验通过后,才会启动主核,执行主核的代码;如果校验失败,则会禁止主核启动,或者限制主核的部分功能和权限。

[0063] 参考图4,为本发明实施例提供的芯片结构示意图。

[0064] 图4为本发明实施例提供的芯片结构400,包括:安全子系统401,主系统402,目标存储器403 以及通信模块404。

[0065] 目标存储器403可以是非易失性存储器,通信模块404可以是邮箱模块。

[0066] 本发明中,安全子系统401通过通信模块404与主系统402通信连接,安全子系统401与目标存储器403通信连接,主系统402与目标存储器403通信连接,安全子系统401与通信模块404之间可以进行读写访问,主系统402与通信模块404之间也可以进行读写访问,安全子系统401与目标存储器403之间可以进行读写访问,而主系统402与目标存储器403之间仅可以进行读访问。

[0067] 参考图5,为本发明实施例提供的非易失性存储器示意图。

[0068] 为实现本发明一些实施例的数据处理方式,对芯片内部结构的读写方式进行调整。

[0069] 安全子系统401和主系统402对目标存储器403的读写权限不同,安全子系统401对

目标存储器403可以进行读取和写入操作,主系统402只能对目标存储器403进行读取操作,无法擦写目标存储器403中的内容。由于安全子系统401是整个芯片的可信根,因此,安全子系统401对目标存储器403的擦写操作是可信的。由于主系统不是可信根,则不能对目标存储器403中的数据进行擦写操作,有效防止了目标存储器403中的数据被干扰或恶意篡改。

[0070] 为实现上述读写权限的改变,对目标存储器403内部结构进行了优化。

[0071] 目标存储器403包括目标存储器控制器4031以及目标存储器主阵列4032。本发明在目标存储器控制器4031内增加一个总线主设备权限控制器4033,可以通过总线实现针对不同系统端访问权限的控制。总线主设备权限控制器4033仅授权安全子系统401对目标存储器403进行擦写操作,禁止主系统402或总线上其他设备对目标存储器403进行擦写操作,主系统402仅可以对目标存储器403进行读操作。

[0072] 参考图6,为本发明实施例提供的应用于芯片的安全子系统的数据处理方法流程示意图。

[0073] 步骤S601,安全子系统接收主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信。

[0074] 在具体实施中,更新流程由主系统(即主核)发起,安全子系统首先需要验证发起者的可信性,并且只执行可信的主体发起的更新请求。更新请求通常通过网络通信或特定的接口进行传输。安全子系统需要解析请求以获取必要的信息,如请求的类型、涉及的数据、更新操作的详细描述等。安全子系统与主系统之间的安全认证可以使用常见的对称或者非对称的加密算法来实现。

[0075] 以银行系统为例,其中主核负责处理日常交易,而安全子系统负责存储敏感数据(如客户身份信息和交易记录)。当主核需要更新某些客户数据时,它会向安全子系统发送数据更新请求。安全子系统在接收到请求后,会按照上述步骤验证主核的可信性,只有在验证通过后才执行更新操作。

[0076] 步骤S602,安全子系统响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入目标存储器。

[0077] 在具体实施中,安全子系统验证主系统可信之后,接收其发送的待处理数据以及相应的第一校验值,并将这些数据写入目标存储器。待处理数据即需要更新或存储的代码,主系统会通过通信接口从外部获取待写入目标存储器的数据,并通过邮箱模块发送到安全子系统。第一校验值即初始的可信校验值,用于验证数据的完整性和准确性。第一校验值通常是通过哈希函数或其他算法计算得出的,它代表数据的某种数字摘要或指纹。

[0078] 需要说明的是,在数据传输和写入过程中,可以采用加密和安全通信协议,以防止数据泄露或被非法截获。如果在写入过程中发生任何错误,如存储器故障或数据传输错误,可以采用相应的错误处理机制,如重试、日志记录或报警。

[0079] 作为一个可选的实施例,安全子系统认证主系统可信之后,需要向主系统发送可信认证结果,以使主系统根据可信认证结果获取待处理数据以及第一校验值。

[0080] 具体地,一旦安全子系统验证主系统为可信,安全子系统会生成一个可信认证结果,并通过安全通道发送给主系统。这个认证结果可以是一个简单的确认消息,也可以包含更详细的信息,如认证的时间戳、有效期或特定的权限标识。在确认其身份和权限后,主系统会从相应的数据源获取待处理的数据以及与之关联的第一校验值。这些数据可能是存储

在主系统本地,也可能是从其他可信的系统或外部数据源获取。

[0081] 作为一个可选的实施例,若安全子系统验证主系统不可信,则终止将待处理数据以及第一校验值写入目标存储器的流程。

[0082] 具体地,如果验证过程中发现主系统的身份、权限或行为不符合预期,或者存在任何异常或安全风险,安全子系统将判定主系统不可信。一旦确定主系统不可信,安全子系统会立即终止将待处理数据以及第一校验值写入目标存储器的流程。这意味着数据不会被传输到目标存储器,也不会进行任何后续的写入操作。通过终止写入流程,可以防止不可信的主系统获取或篡改敏感数据,从而保护数据的机密性和完整性。及时识别和拒绝不可信的系统端,可以降低潜在的系统风险和安全漏洞。

[0083] 作为一个可选的实施例,安全子系统将待处理数据以及第一校验值写入目标存储器之前,需要将目标存储器中的数据的数据状态标记为无效状态;其中,无效状态用于表征目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0084] 具体地,当系统决定开始更新代码时,首先会把代码是否有效的标志设置为无效。这样做是为了确保在更新过程中,即使系统意外重启或发生其他中断,也不会尝试执行不完整的代码。在更新之前,可以选择备份非易失性存储器中的旧代码。这样做可以提供一个恢复点,以防更新过程中出现问题。将新的代码片段逐步写入非易失性存储器。如果在代码更新完成之前,系统尝试执行非易失性存储器中的不完整代码,可能会导致不可预测的行为、系统崩溃甚至数据损坏。因此,设置代码是否有效的标志是一个重要的安全措施。执行时部分功能受限可以理解为即使某些系统组件或进程尝试访问或执行这些数据,它们所能执行的操作也将受到限制。

[0085] 步骤S603,安全子系统根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配。

[0086] 在数据处理和存储的流程中,对数据的完整性和准确性进行校验是至关重要的。

[0087] 作为一个可选的实施例,安全子系统在接收到主系统发送的待处理数据以及第一校验值后,使用预先存储的数据校验密钥对这些数据进行校验,生成新的数据校验值(即第二校验值)。数据校验密钥是预先存储在一个安全且可靠的地方的密钥信息,用于对数据进行校验和验证。在进行校验之前,系统需要安全地获取这个密钥,确保密钥的保密性和完整性。使用获取到的数据校验密钥,对待处理数据进行校验计算。校验计算通常涉及到一种或多种加密算法或哈希函数,这些算法或函数能够将数据转换成一个唯一的校验值(即第二校验值)。第二校验值可以理解为是待处理数据在当前状态下的数字指纹,代表了数据的完整性和内容。进一步地,系统会将第一校验值与第二校验值进行匹配,以确定待处理数据在传输过程中的准确性和完整性。

[0088] 作为一个可选的实施例,安全子系统确定主系统可信后,主系统可以向安全子系统发起更新通知,以通知安全子系统将待处理数据以及第一校验值写入目标存储器。

[0089] 步骤S604,安全子系统响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新。

[0090] 作为一个可选的实施例,如果这两个校验值完全匹配,那么可以认为待处理数据在传输过程中未被篡改,是完整和准确的。

[0091] 具体地,通过校验值的匹配确认,可以大大提高数据传输的可靠性和安全性。校验值的计算通常基于复杂的加密算法或哈希函数,保证了校验值的唯一性和难以伪造性。

[0092] 作为一个可选的实施例,如果这两个校验值完全匹配,可以将目标存储器中的数据的数据状态标记为有效状态;其中,有效状态用于表征目标存储器中的数据允许被执行。

[0093] 具体地,当确认待处理数据的完整性后,为了进一步保证系统的安全性和数据的可用性,可以将目标存储器中的数据状态标记为有效状态。这个有效状态表明目标存储器中的数据是完整、准确且允许被执行的。

[0094] 作为一个可选的实施例,如果第一校验值与第二校验值不匹配,则将目标存储器中的数据的数据状态维持为无效状态;其中,无效状态用于表征目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0095] 如果不匹配,则表明数据可能在传输过程中被篡改或损坏,需要进一步处理或拒绝接收。当第一校验值与第二校验值不匹配时,应该将目标存储器中的数据的数据状态维持为无效状态。无效状态明确地指示该数据不应被执行,从而防止了潜在的安全风险和损坏。通过维持无效状态,系统可以防止执行可能已损坏或被篡改的数据,从而避免潜在的安全风险和错误,确保了只有经过验证和确认完整性的数据才会被执行,提高了系统的安全性和数据的可靠性。

[0096] 作为一个可选的实施例,当发现校验值不匹配时,系统应记录相应的错误日志,包括不匹配的校验值、数据接收时间、来源等信息,以便后续审计和故障排查。根据系统的安全策略,还可以触发警报或通知管理员,以便采取进一步的措施。

[0097] 作为一个可选的实施例,数据更新指令可以但不限于包括数据更新的标识符、时间戳或版本号等信息,使主系统能够明确知道目标存储器中的数据已经完成更新。数据更新指令还可以包含关于更新数据的详细描述,如数据的大小、类型或用途等,以便主系统根据需要进行后续处理。安全子系统通过发送数据更新指令,能够确保主系统在数据完整性得到验证后及时了解数据的更新状态。

[0098] 作为一个可选的实施例,安全子系统响应于确定目标芯片的启动信息,则读取目标存储器中的数据的数据状态,若确定目标存储器中的数据状态为有效状态,则控制主系统启动,并控制主系统执行目标存储器中的数据。

[0099] 作为一个可选的实施例,安全子系统响应于目标存储器中的数据状态为无效状态,则禁止主系统执行目标存储器中的数据,或,控制主系统执行目标存储器中的部分数据。

[0100] 具体地,系统检查读取到的数据状态。如果数据状态为有效状态,表明数据是完整且未被篡改的,允许被执行;如果数据状态为无效状态,则数据不应被执行。通过读取和验证目标存储器中的数据状态,系统能够确保只有在数据完整且未被篡改的情况下才执行操作,从而提高了系统的安全性和数据的可靠性。且本发明从芯片硬件上保证对目标存储器进行擦写操作的主体是可信的,并且在什么时间对非易失性存储器进行擦写操作完全由安全子系统控制,所以,只需要在代码或者数据更新时由安全子系统进行校验,而不需要每次启动时都对代码或者数据进行校验,节约了安全启动的时间。

[0101] 参考图7,为本发明实施例提供的应用于芯片的主系统的数据处理流程示意图。

[0102] 步骤S701,主系统向安全子系统发送数据更新请求。

[0103] 步骤S702,主系统接收安全子系统发送的可信认证结果,根据可信认证结果获取待处理数据以及第一校验值。

[0104] 步骤S703,主系统接收数据更新指令。

[0105] 在步骤S701~步骤S702中,主系统需要获取最新的数据以执行相关任务或操作,因此向安全子系统发送数据更新请求。该请求可以包含主系统的标识符、所需数据的类型或范围等信息,以便安全子系统正确响应。安全子系统在接收到数据更新请求后,根据数据更新请求验证主系统是否可信,若可信,安全子系统将可信认证结果发送给主系统。主系统开始获取待处理数据和第一校验值,并将待处理数据和第一校验值发送到安全子系统。当安全子系统对写入目标存储器的数据校验成功后,向主系统发送数据更新指令,数据更新指令表明目标存储器中的数据已经完成更新,并且允许主系统执行这些数据。主系统接收到数据更新指令后,可以开始加载和执行这些数据,以完成其预定任务或操作。

[0106] 参考图8,为本发明实施例提供的数据处理方法应用于安全子系统以及主系统的交互流程示意图。

[0107] 作为一个可选的实施例,更新流程由主系统发起,安全子系统首先需要验证发起者的可信性。如果认证失败,直接退出更新流程,防止非可信主体篡改非易失性存储器内容。如果认证成功,则会开始执行代码更新。由于代码更新全部完成前,存储在目标存储器中的只是不完整的代码,所以认为是无效的代码。因此,在代码更新前,会先把代码是否有效的标志设置为无效。在代码更新的过程中,主系统会通过通信接口从外部获取待写入非易失性存储器的数据,并通过邮箱模块发送到安全子系统。安全子系统收到信息后,会读取待写入的数据,写入非易失性存储器中。这个步骤可能会重复多次,直到所有数据都更新完成。进一步地,安全子系统将数据的校验值,写入非易失性存储器,读取密钥,进行校验。如果校验通过,则会把代码有效标志设置为有效,通知主核结果,完成更新。如果校验不通过,则更新不成功,代码有效标志保持为无效。

[0108] 由于非易失性存储器的内容的修改的时间和内容的有效性的检查都由可以信赖的安全子系统来完成,所以,其内容的修改是安全可控的,不会被非可信的主体随意篡改。因此,在芯片启动的时候,不需要再进行代码的安全校验,只需要读取代码是否有效的标志即可。

[0109] 参考图9,为本发明实施例提供的芯片代码更新流程示意图。

[0110] 系统启动后,会先检查代码有效标志,如果代码有效,则启动主系统,执行代码;如果代码无效,则禁止主系统启动,或者限制主系统的部分功能和权限。由于安全启动时省去了对代码进行安全校验的步骤,只需要读取代码有效标志,可以在保证代码可信与正确的同时,大大减小启动时间,提升启动速度。

[0111] 从上面所述可以看出,本发明提供的应用于芯片的数据处理方法,通过安全子系统对主系统的数据更新请求进行验证,以确保主系统是可信的,增强了系统的安全性,防止了恶意或未经授权的更新,进一步地,由持有可信密钥的安全子系统写入并校验待处理数据,确保数据在写入过程中没有被篡改,保证了数据的完整性,使得每次更新都是可靠和准确的。通过安全子系统与主系统的协同工作,确保整个数据更新流程更加有序和可靠,主核无需在每次启动时都对数据进行校验,节约了数据更新时间,且减少因数据不一致或错误

更新而导致的系统故障,增强了系统的稳定性和可靠性。

[0112] 需要说明的是,本发明实施例的方法可以由单个设备执行,例如一台计算机或服务器等。本实施例的方法也可以应用于分布式场景下,由多台设备相互配合来完成。在这种分布式场景的情况下,这多台设备中的一台设备可以只执行本发明实施例的方法中的某一个或多个步骤,这多台设备相互之间会进行交互以完成所述的方法。

[0113] 需要说明的是,上述对本发明的一些实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于上述实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0114] 基于同一发明构思,与上述任意实施例提供的方法相对应的,本发明还提供了一种芯片。

[0115] 参考图10,为本发明实施例提供的一种芯片示意图。

[0116] 所述装置包括:所述芯片包括安全子系统1001、主系统1002和目标存储器1003,所述安全子系统1001与所述目标存储器1003进行读写访问,所述主系统1002与所述目标存储器1003进行读访问;

[0117] 所述安全子系统1001被配置为:

[0118] 接收所述主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信;

[0119] 响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入所述目标存储器;

[0120] 根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配;

[0121] 响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新。

[0122] 可选的,所述安全子系统1001,还被配置为:

[0123] 向所述主系统发送可信认证结果,以使所述主系统根据所述可信认证结果获取所述待处理数据以及所述第一校验值。

[0124] 可选的,所述安全子系统1001,还被配置为:

[0125] 响应于所述主系统不可信,终止将所述待处理数据以及所述第一校验值写入目标存储器的流程。

[0126] 可选的,所述安全子系统1001,还被配置为:

[0127] 将所述目标存储器中的数据的数据状态标记为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0128] 可选的,所述安全子系统1001,还被配置为:

[0129] 将所述目标存储器中的数据的数据状态标记为有效状态;其中,所述有效状态用于表征所述目标存储器中的数据允许被执行。

[0130] 可选的,所述安全子系统1001,还被配置为:

[0131] 响应于所述第一校验值与所述第二校验值不匹配,则将所述目标存储器中的数据

的数据状态维持为无效状态;其中,所述无效状态用于表征所述目标存储器中的数据禁止被执行或者执行时部分功能受限。

[0132] 可选的,所述主系统1002,还被配置为:

[0133] 响应于确定所述芯片的启动信息,则读取所述目标存储器中的数据的数据状态;

[0134] 响应于所述目标存储器中的数据状态为有效状态,读取并执行所述目标存储器中的数据。

[0135] 可选的,所述主系统1002,还被配置为:

[0136] 响应于所述目标存储器中的数据状态为无效状态,禁止执行所述目标存储器中的数据,或,执行所述目标存储器中的部分数据。

[0137] 根据本发明实施例提供的一种芯片,安全子系统用于接收主系统发送的数据更新请求,根据所述数据更新请求验证所述主系统是否可信,响应于所述主系统可信,接收所述主系统发送的待处理数据以及第一校验值,将所述待处理数据以及所述第一校验值写入目标存储器,根据预先存储的数据校验密钥对所述待处理数据进行校验,生成第二校验值,确定所述第一校验值与所述第二校验值是否匹配,响应模块用于响应于所述第一校验值与所述第二校验值匹配,向所述主系统发送数据更新指令;其中,所述数据更新指令用于表征所述目标存储器中的数据已经完成更新。由此,该芯片通过安全子系统负责数据的更新和校验,并且在更新时及时更新代码是否有效的标志,芯片在启动时只需读取该标志,而无需对整个代码进行校验。这大大减少了启动时间,提高了系统的实时性,特别是在代码量大的系统上,这种优化效果更加明显。如果检测到数据被篡改或校验失败,安全子系统能够立即采取相应措施,如禁止主系统启动或限制其功能,从而及时阻止非法操作。这种实时防护机制提高了芯片的安全性,并能够在发生安全问题时迅速做出响应。

[0138] 为了描述的方便,描述以上系统时以功能分为各种模块分别描述。当然,在实施本发明时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

[0139] 上述实施例的系统用于实现前述任一实施例中相应的数据处理方法,并且具有相应的方法实施例的有益效果,在此不再赘述。

[0140] 基于同一发明构思,与上述任意实施例所述的数据处理方法相对应的,本发明还提供了一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现上任意一实施例所述的数据处理方法。

[0141] 图11示出了本实施例所提供的一种更为具体的电子设备硬件结构示意图,该设备可以包括:处理器1110、存储器1120、输入/输出接口1130、通信接口1140和总线1150。其中处理器1110、存储器1120、输入/输出接口1130和通信接口1140通过总线1150实现彼此之间在设备内部的通信连接。

[0142] 处理器1110可以采用通用的CPU(Central Processing Unit,中央处理器)、微处理器、应用专用集成电路(Application Specific Integrated Circuit,ASIC)、或者一个或多个集成电路等方式实现,用于执行相关程序,以实现本说明书实施例所提供的技术方案。

[0143] 存储器1120可以采用ROM(Read Only Memory,只读存储器)、RAM(Random Access Memory,随机存取存储器)、静态存储设备,动态存储设备等形式实现。存储器1120可以存储操作系统和其他应用程序,在通过软件或者固件来实现本说明书实施例所提供的技术方案

时,相关的程序代码保存在存储器1120中,并由处理器1110来调用执行。

[0144] 输入/输出接口1130用于连接输入/输出模块,以实现信息输入及输出。输入/输出模块可以作为组件配置在设备中(图中未示出),也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等,输出设备可以包括显示器、扬声器、振动器、指示灯等。

[0145] 通信接口1140用于连接通信模块(图中未示出),以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式(例如USB、网线等)实现通信,也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信。

[0146] 总线1150包括一通路,在设备的各个组件(例如处理器1110、存储器1120、输入/输出接口1130和通信接口1140)之间传输信息。

[0147] 需要说明的是,尽管上述设备仅示出了处理器1110、存储器1120、输入/输出接口1130、通信接口1140以及总线1150,但是在具体实施过程中,该设备还可以包括实现正常运行所必需的其他组件。此外,本领域的技术人员可以理解的是,上述设备中也可以仅包含实现本说明书实施例方案所必需的组件,而不必包含图中所示的全部组件。

[0148] 上述实施例的电子设备用于实现前述任一实施例中相应的数据处理方法,并且具有相应的数据处理方法实施例的有益效果,在此不再赘述。

[0149] 基于同一发明构思,与上述任意实施例所述的数据处理方法相对应的,本发明还提供了一种非暂态计算机可读存储介质,所述非暂态计算机可读存储介质存储计算机指令,所述计算机指令用于使所述计算机执行如上任一实施例所述的数据处理方法。

[0150] 上述非暂态计算机可读存储介质可以是计算机能够存取的任何可用介质或数据存储设备,包括但不限于磁性存储器(例如软盘、硬盘、磁带、磁光盘(MO)等)、光学存储器(例如CD、DVD、BD、HVD等)、以及半导体存储器(例如ROM、EPROM、EEPROM、非易失性存储器(NAND FLASH)、固态硬盘(SSD))等。

[0151] 上述实施例的存储介质存储的计算机指令用于使所述计算机执行如上示例性方法部分中任一实施例所述的数据处理方法,并且具有相应的方法实施例的有益效果,在此不再赘述。

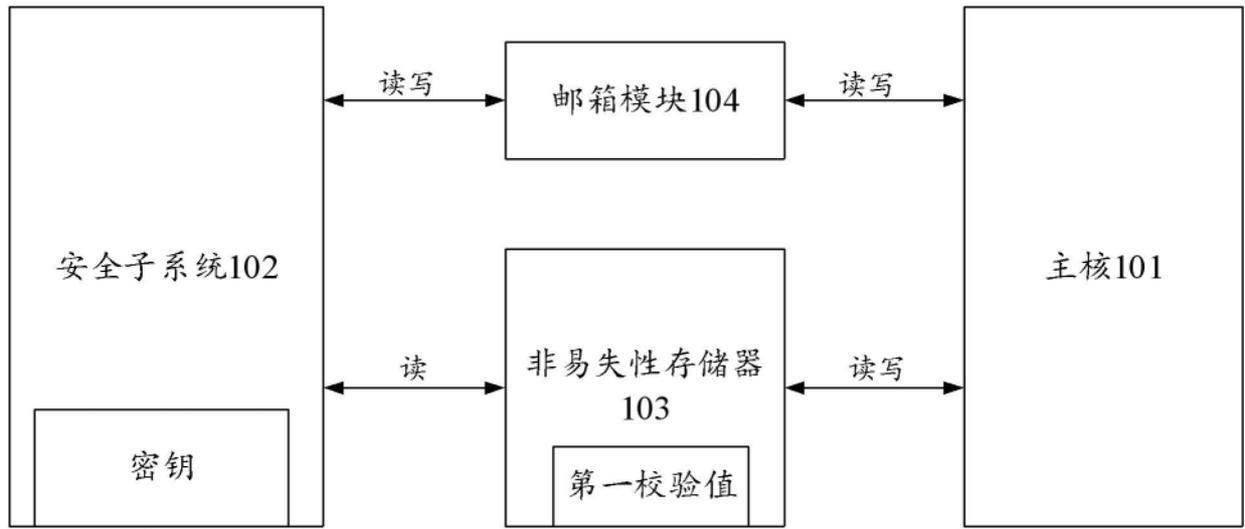
[0152] 此外,尽管在附图中以特定顺序描述了本发明方法的操作,但是,这并非要求或者暗示必须按照该特定顺序来执行这些操作,或是必须执行全部所示的操作才能实现期望的结果。相反,流程图中描绘的步骤可以改变执行顺序。附加地或备选地,可以省略某些步骤,将多个步骤合并为一个步骤执行,和/或将一个步骤分解为多个步骤执行。

[0153] 应当理解,本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中,多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如,如果用硬件来实现,和在另一实施方式中一样,可用本领域公知的下列技术中的任一项或他们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路,具有合适的组合逻辑门电路的专用集成电路,可编程门阵列(PGA),现场可编程门阵列(FPGA)等。

[0154] 需要说明的是,除非另外定义,本发明实施例使用的技术术语或者科学术语应当为本发明所属领域内具有一般技能的人士所理解的通常意义。本发明实施例中使用的“第一”、“第二”以及类似的词语并不表示任何顺序、数量或者重要性,而只是用来区分不同的

组成部分。“包括”或者“包含”等类似的词语意指出现该词前面的元件或者物件涵盖出现在该词后面列举的元件或者物件及其等同,而不排除其他元件或者物件。“连接”或者“相连”等类似的词语并非限定于物理的或者机械的连接,而是可以包括电性的连接,不管是直接的还是间接的。“上”、“下”、“左”、“右”等仅用于表示相对位置关系,当被描述对象的绝对位置改变后,则该相对位置关系也可能相应地改变。

[0155] 虽然已经参考若干具体实施方式描述了本发明的精神和原理,但是应该理解,本发明并不限于所公开的具体实施方式,对各方面的划分也不意味着这些方面中的特征不能组合以进行受益,这种划分仅是为了表述的方便。本发明旨在涵盖所附权利要求的精神和范围内所包括的各种修改和等同布置。所附权利要求的范围符合最宽泛的解释,从而包含所有这样的修改及等同结构和功能。



100

图1

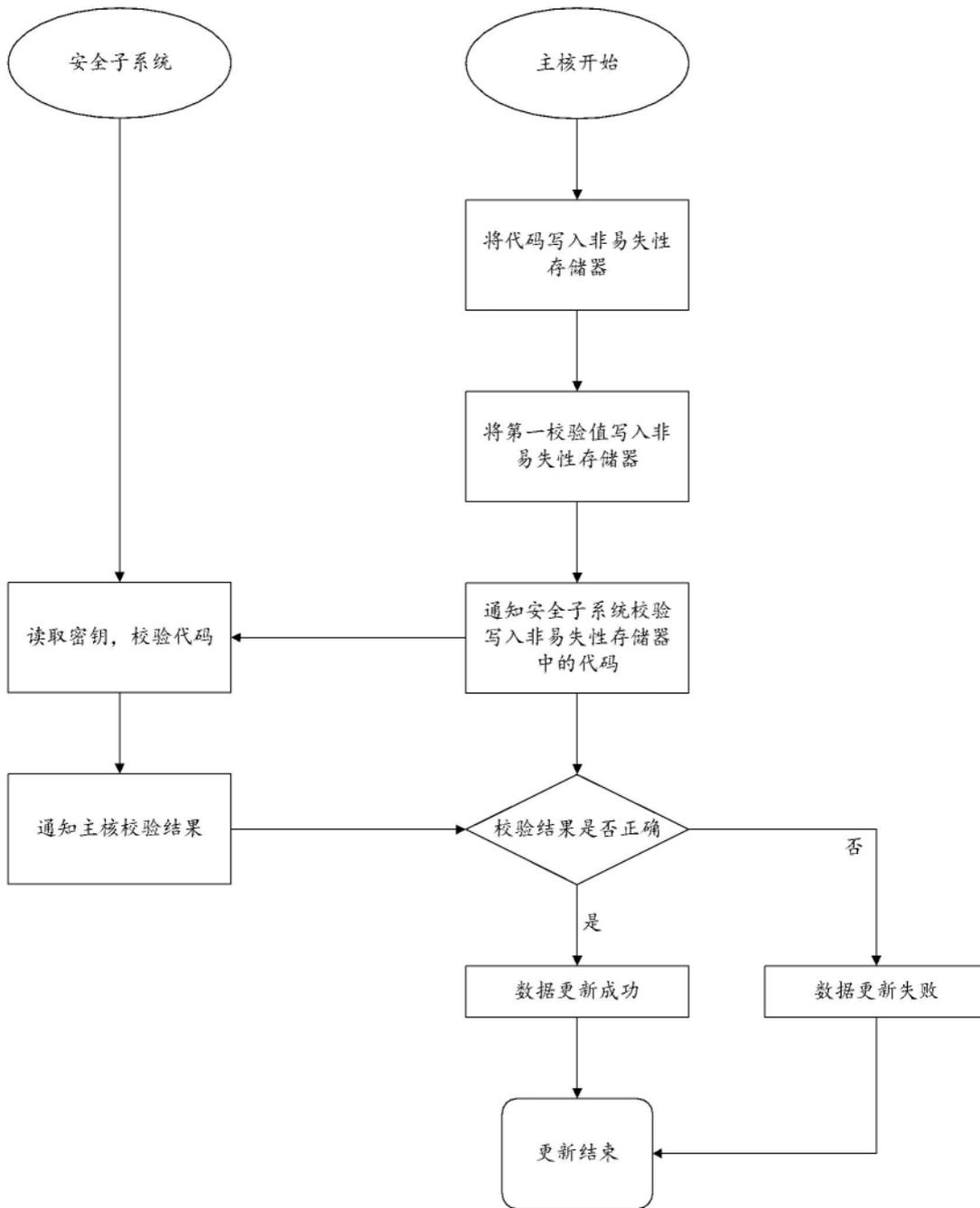


图2

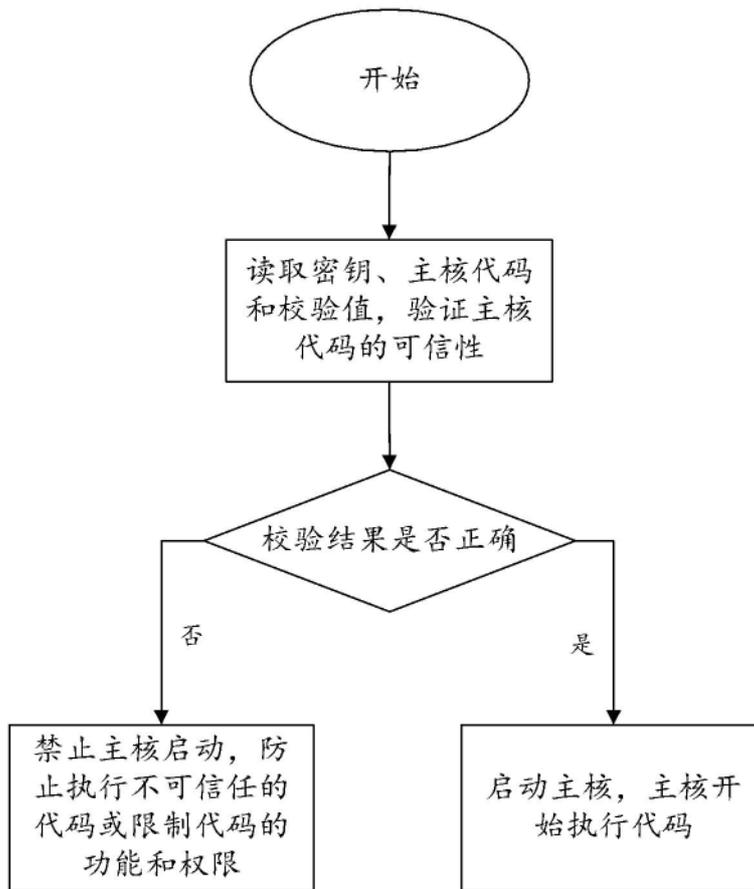
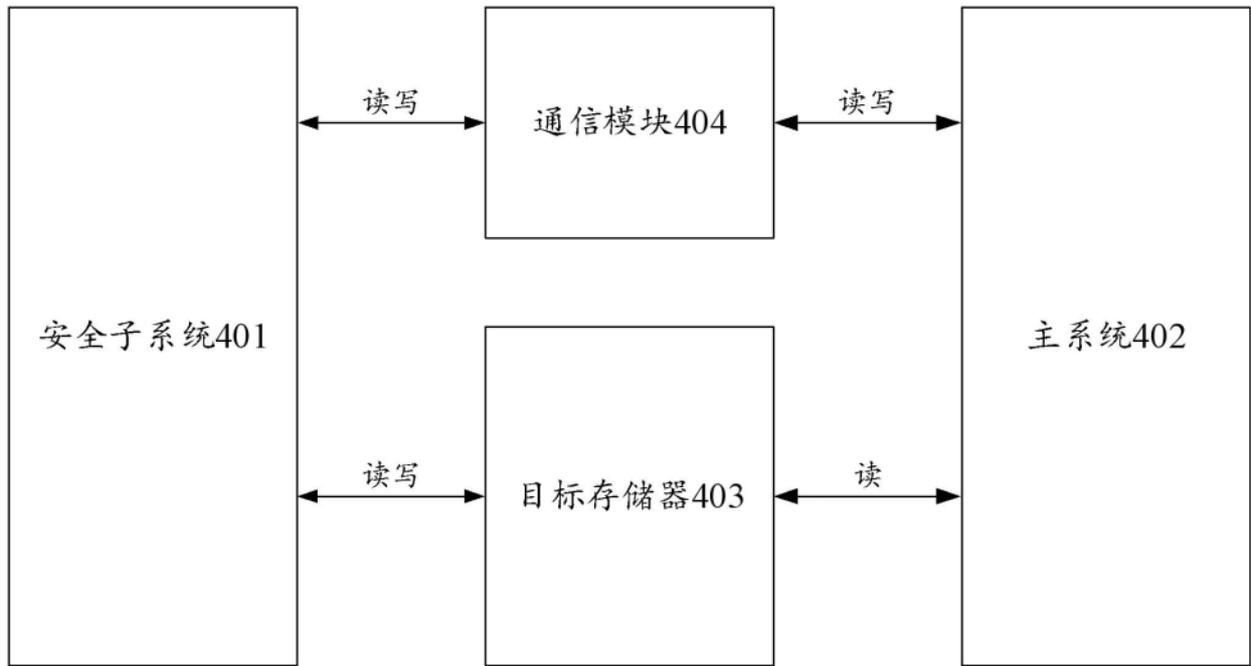


图3



400

图4

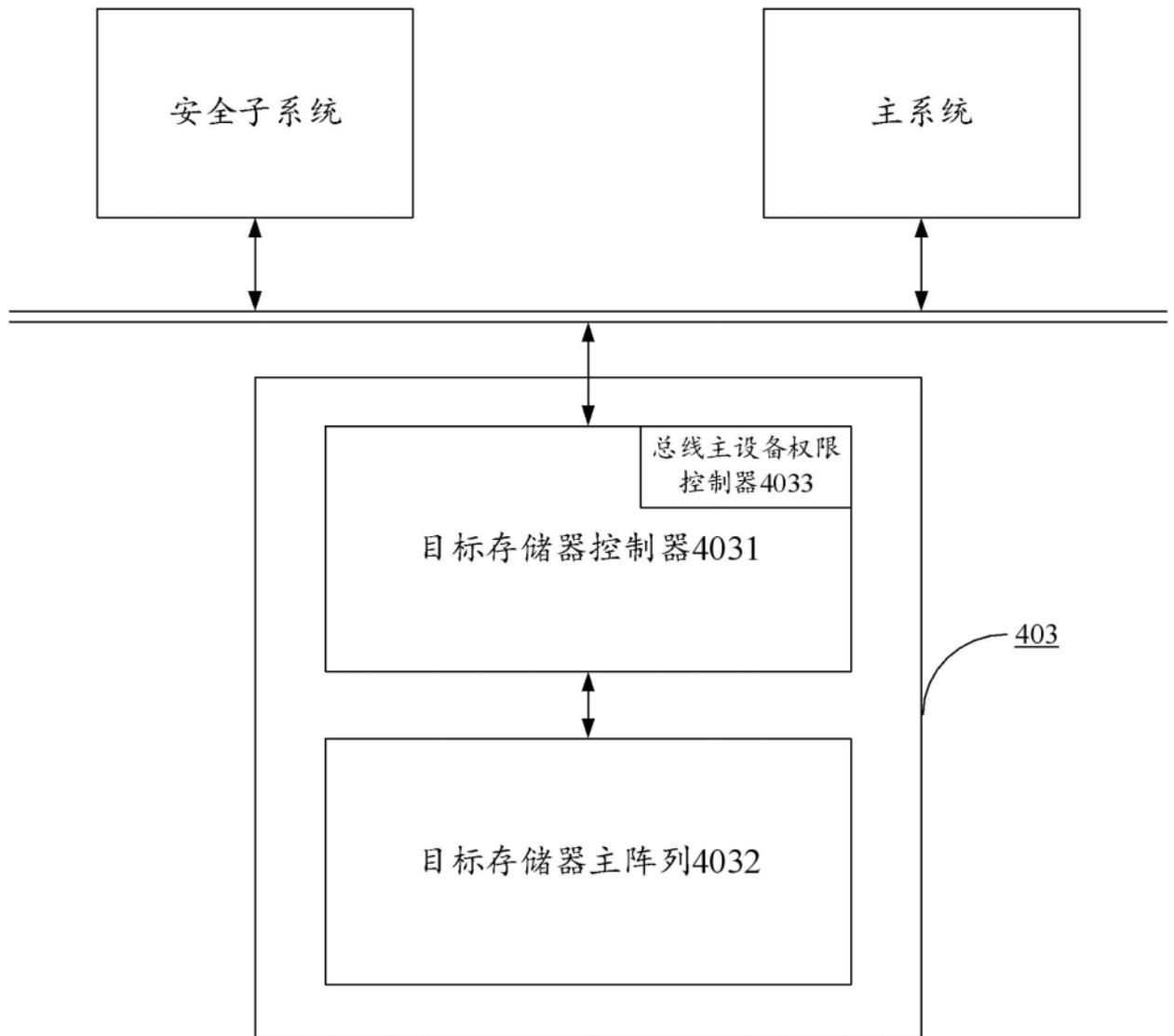


图5

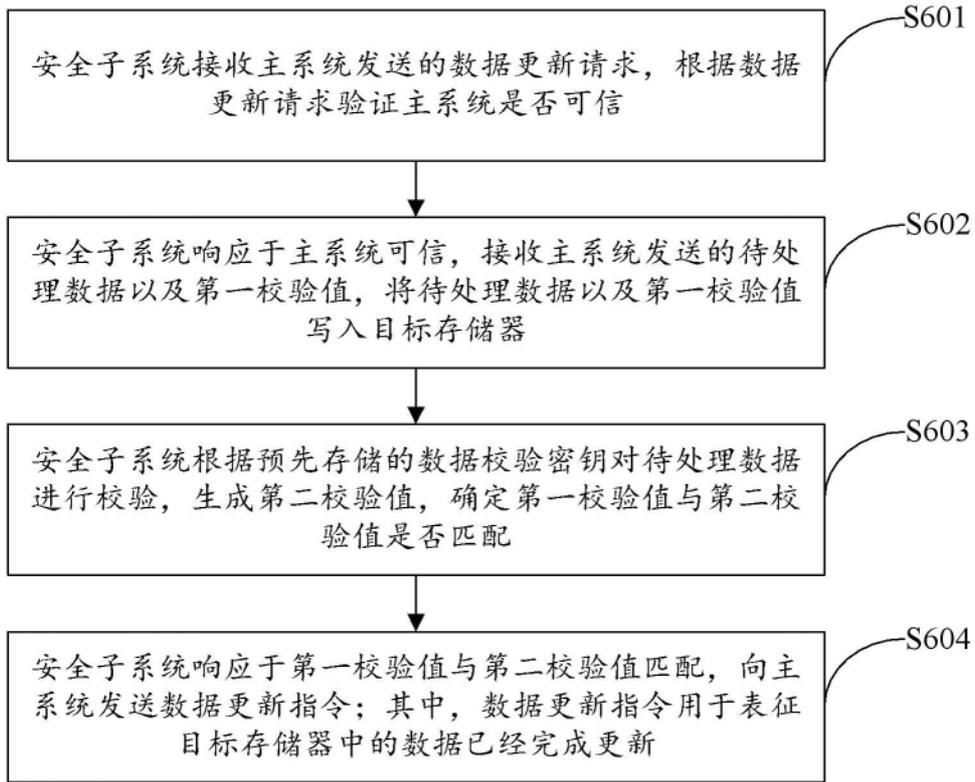


图6

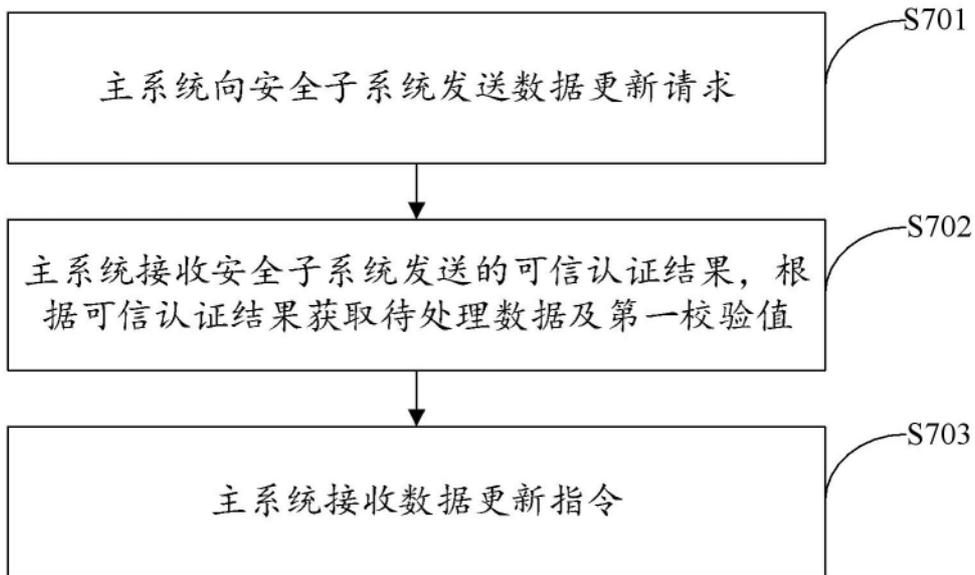


图7

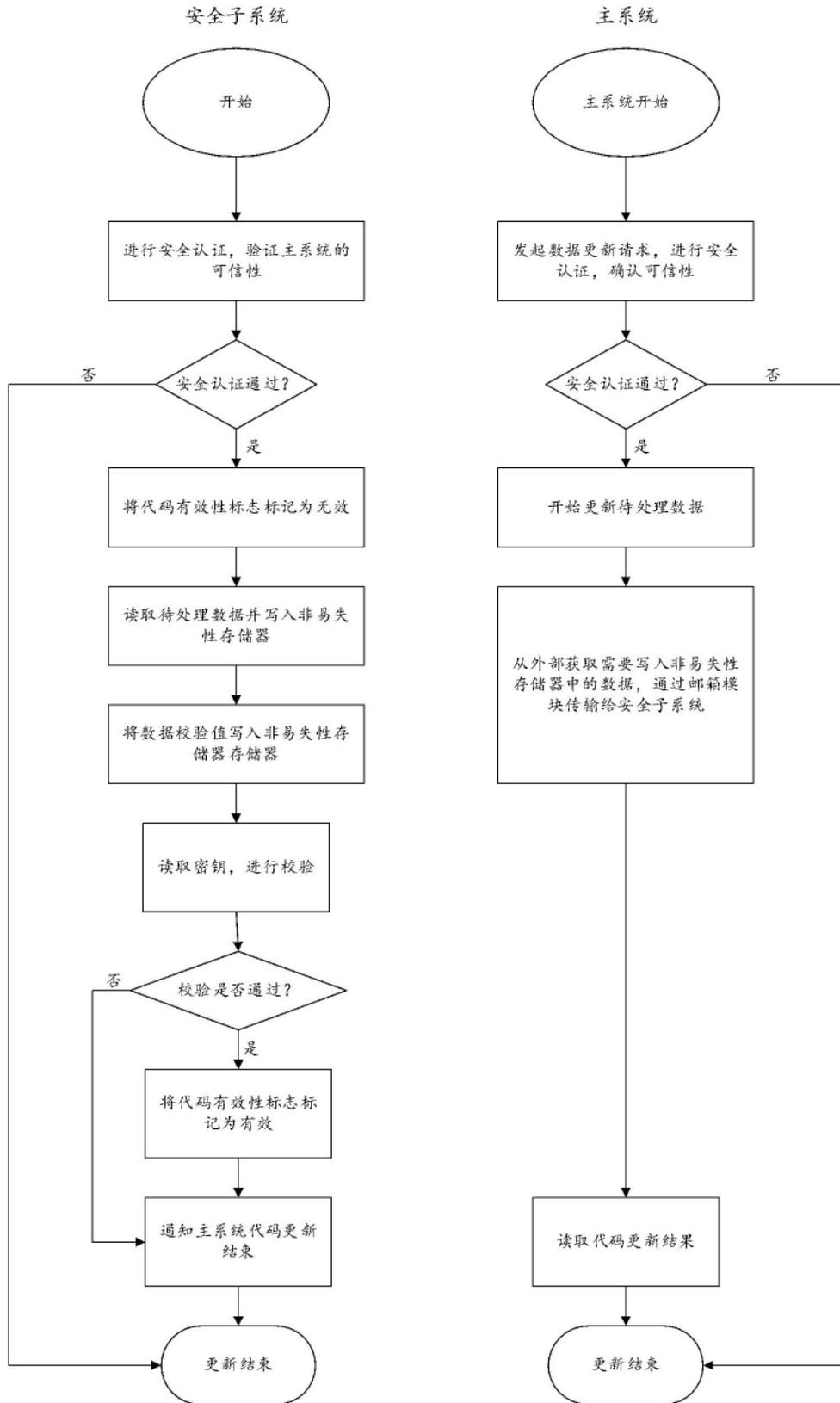


图8

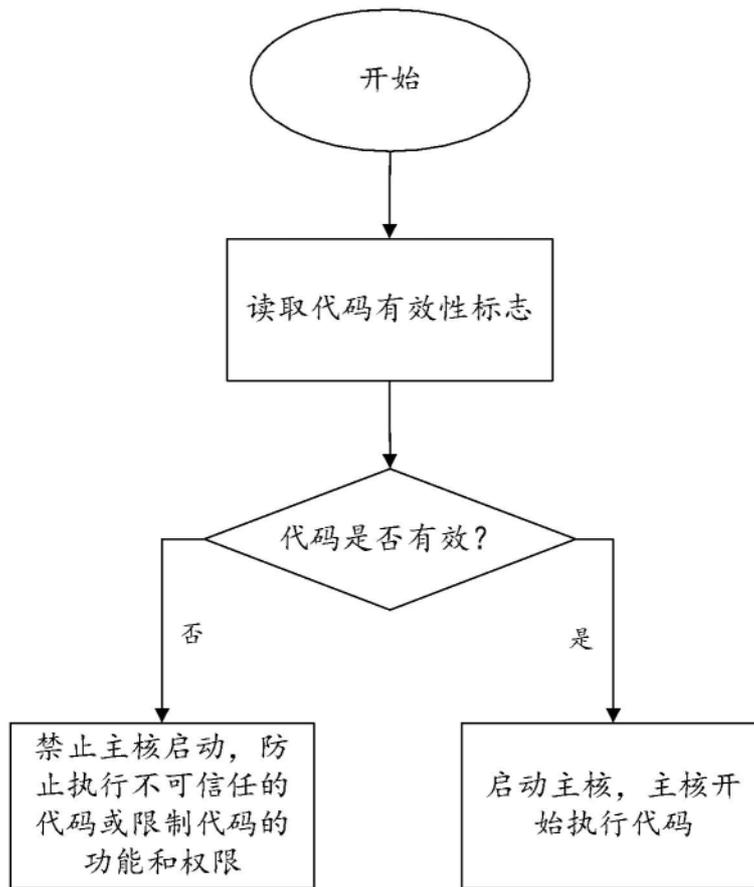


图9

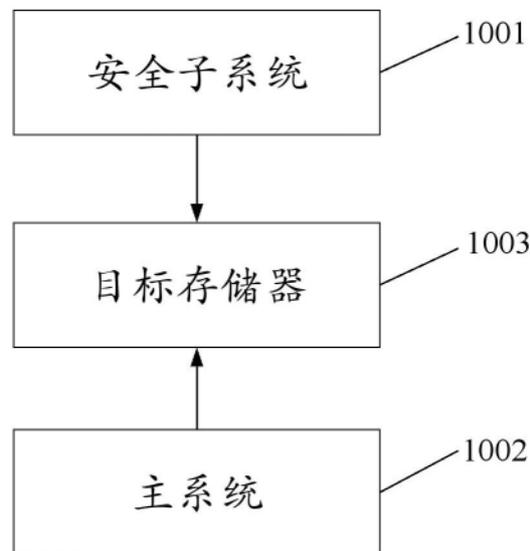


图10

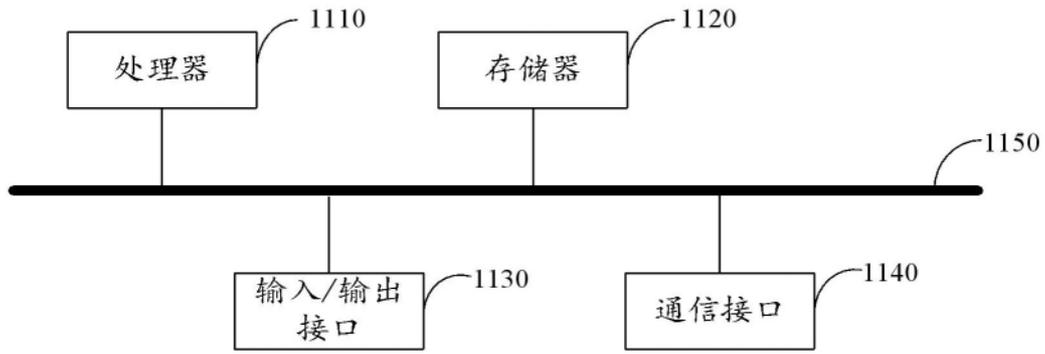


图11