(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 113886834 A
(43)申请公布日 2022.01.04

(21)申请号 202111150136.7

(22)申请日 2021.09.29

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区桃源街道学苑大道1088号

(72)发明人 张锋巍 宁振宇 邓韵杰 王晨旭 刘世晴 于顺昌

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 廖慧贤

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/62(2013.01)
G06F 9/445(2018.01)

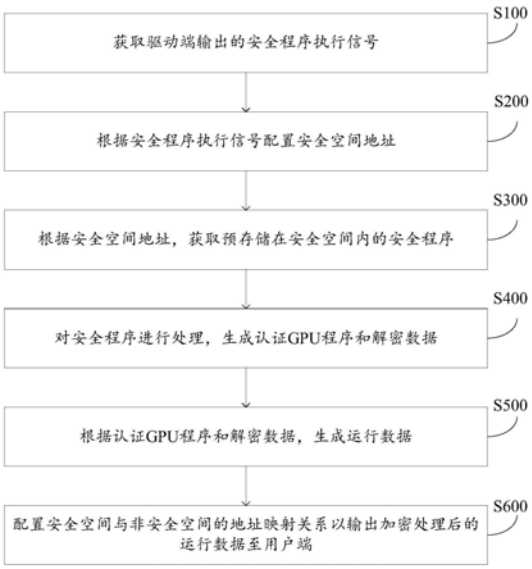
权利要求书2页 说明书7页 附图3页

(54)发明名称

基于ARM架构的GPU可信执行方法、系统、设备及存储介质

(57)摘要

本发明公开了一种基于ARM架构的GPU可信执行方法、系统、设备及存储介质，属可信执行技术领域。该方法包括：获取驱动端输出的安全程序执行信号；根据安全程序执行信号配置安全空间地址；根据安全空间地址，获取预存储在安全空间内的安全程序；对安全程序进行处理，生成认证GPU程序和解密数据；根据认证GPU程序和解密数据，生成运行数据；配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至用户端。该方法无须修改GPU硬件，便能在基于ARM架构的设备中实现GPU可信执行，提高了运行兼容性和安全性。



CN 113886834 A

1.基于ARM架构的GPU可信执行方法,其特征在于,包括:

获取驱动端输出的安全程序执行信号;

根据所述安全程序执行信号配置安全空间地址;

根据所述安全空间地址,获取预存储在安全空间内的安全程序;

对所述安全程序进行处理,生成认证GPU程序和解密数据;

根据所述认证GPU程序和所述解密数据,生成运行数据;

配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至用户端。

2.根据权利要求1所述的基于ARM架构的GPU可信执行方法,其特征在于,所述获取驱动端输出的安全程序执行信号之前,该方法包括:

通过所述用户端获取用户数据和GPU程序;

所述用户端根据所述用户数据和所述GPU程序,生成所述安全程序;

将所述安全程序存储至所述安全空间。

3.根据权利要求1所述的基于ARM架构的GPU可信执行方法,其特征在于,所述获取驱动端输出的安全程序执行信号之前,还包括:

通过GPU输出当前任务结束信号至所述驱动端;

接收所述驱动端根据所述当前任务结束信号输出的安全程序执行信号。

4.根据权利要求1所述的基于ARM架构的GPU可信执行方法,其特征在于,所述对所述安全程序进行处理,生成认证GPU程序和解密数据,包括:

根据所述安全程序,得到对应的用户数据和GPU程序;

根据对所述GPU程序的完整性检验,生成所述认证GPU程序;

根据获取到的解密算法对所述用户数据进行解密处理,生成所述解密数据。

5.根据权利要求1至4任一项所述的基于ARM架构的GPU可信执行方法,其特征在于,所述根据所述认证GPU程序和所述解密数据,生成运行数据之后,该方法还包括:

根据所述运行数据,生成安全程序结束信号。

6.根据权利要求5所述的GPU可信执行方法,其特征在于,所述配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至所述用户端之前,该方法包括:

根据所述安全程序结束信号,得到加密算法;

根据所述加密算法对所述运行数据进行加密处理,生成加密处理后的运行数据。

7.根据权利要求6所述的GPU可信执行方法,其特征在于,所述配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至所述用户端,该方法包括:

获取所述加密处理后的运行数据,并根据所述加密处理后的运行数据,配置安全空间与非安全空间的地址映射关系;

根据所述地址映射关系,调取所述安全空间内的加密处理后的运行数据至所述非安全空间,以使所述驱动端获取加密处理后的运行数据并将所述加密处理后的运行数据发送至所述用户端。

8.基于ARM架构的GPU可信执行系统,其特征在于,包括:

基于ARM架构的可信固件,用于获取驱动端输出的安全程序执行信号;根据所述安全程序执行信号配置安全空间地址;根据所述安全空间地址,获取预存储在安全空间内的安全程序;对所述安全程序进行处理,生成认证GPU程序和解密数据;配置安全空间与非安全空

间的地址映射关系以输出加密处理后的运行数据至用户端；

GPU，所述GPU连接所述基于ARM架构的可信固件，所述GPU用于根据所述认证GPU程序和所述解密数据，生成运行数据。

9.基于ARM架构的GPU可信执行设备，其特征在于，包括：

至少一个处理器，以及

与所述至少一个处理器通信连接的存储器，其中，

所述存储器存储有指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器执行所述指令时实现如权利要求1至7任一项所述的基于ARM架构的GPU可信执行方法。

10.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有计算机可执行指令，可用于执行如权利要求1至7任一项所述的基于ARM架构的GPU可信执行方法。

基于ARM架构的GPU可信执行方法、系统、设备及存储介质

技术领域

[0001] 本发明涉及可信执行技术领域，尤其是一种基于ARM架构的GPU可信执行方法、装置、系统及存储介质。

背景技术

[0002] 目前，相关技术中的GPU的可信执行技术在应用于不同的终端设备(如应用于ARM架构下的智能手机设备等等)时，往往需要对GPU硬件做出修改，这一方式常常会存在兼容性问题，影响运行安全性。因此，如何提供一种无须修改GPU硬件即可实现在ARM架构下的GPU可信执行技术，以提高运行安全性和兼容性，成为亟待解决的问题。

发明内容

[0003] 本发明旨在至少解决现有技术中存在的技术问题之一。为此，本发明提出一种基于 ARM架构的GPU可信执行方法，能够实现无须修改GPU硬件，即可实现在ARM架构下的 GPU可信执行技术，以提高运行安全性和兼容性。

[0004] 本发明还提出一种基于ARM架构的GPU可信执行系统。

[0005] 本发明还提出一种基于ARM架构的GPU可信执行设备。

[0006] 本发明还提出一种计算机可读存储介质。

[0007] 根据本发明的第一方面实施例的基于ARM架构的GPU可信执行方法，包括：

[0008] 获取驱动端输出的安全程序执行信号；

[0009] 根据所述安全程序执行信号配置安全空间地址；

[0010] 根据所述安全空间地址，获取预存储在安全空间内的安全程序；

[0011] 对所述安全程序进行处理，生成认证GPU程序和解密数据；

[0012] 根据所述认证GPU程序和所述解密数据，生成运行数据；

[0013] 配置安全空间与非安全空间的地址映射关系以输出所述加密处理后的运行数据至所述用户端。

[0014] 根据本发明实施例的基于ARM架构的GPU可信执行方法，至少具有如下有益效果：本方法通过获取安全程序执行信号为安全程序配置安全空间，并通过读取安全空间对应的安全空间地址，获取存储在安全空间的安全程序。通过对安全程序进行处理，获取认证的GPU程序和解密数据。根据认证GPU程序和解密数据，生成运行数据，并对安全空间地址进行释放，以使加密处理后的运行数据可以被释放到非安全空间，从而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储和安全运行，从而实现了在基于ARM架构的设备中完成安全程序的可信执行，提高了GPU可信执行技术的兼容性和运行安全性。

[0015] 根据本发明的一些实施例，所述获取驱动端输出的安全程序执行信号之前，该方法包括：

[0016] 通过所述用户端获取用户数据和GPU程序；

[0017] 所述用户端根据所述用户数据和所述GPU程序，生成所述安全程序；

[0018] 将所述安全程序存储至所述安全空间。

[0019] 根据本发明的一些实施例，所述获取驱动端输出的安全程序执行信号之前，还包括：

[0020] 通过GPU输出当前任务结束信号至所述驱动端；

[0021] 接收所述驱动端根据所述当前任务结束信号输出的安全程序执行信号。

[0022] 根据本发明的一些实施例，所述对所述安全程序进行处理，生成认证GPU程序和解密数据，包括：

[0023] 根据所述安全程序，得到对应的用户数据和GPU程序；

[0024] 根据对所述GPU程序的完整性检验，生成所述认证GPU程序；

[0025] 根据获取到的解密算法对所述用户数据进行解密处理，生成所述解密数据。

[0026] 根据本发明的一些实施例，所述根据所述认证GPU程序和所述解密数据，生成运行数据之后，该方法还包括：

[0027] 根据所述运行数据，生成安全程序结束信号。

[0028] 根据本发明的一些实施例，所述配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至所述用户端之前，该方法包括：

[0029] 根据所述安全程序结束信号，得到加密算法；

[0030] 根据所述加密算法对所述运行数据进行加密处理，生成加密处理后的运行数据。

[0031] 根据本发明的一些实施例，所述配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至所述用户端，该方法包括：

[0032] 获取所述加密处理后的运行数据，并根据所述加密处理后的运行数据，配置安全空间与非安全空间的地址映射关系；

[0033] 根据所述地址映射关系，调取所述安全空间内的加密处理后的运行数据至所述非安全空间，以使所述驱动端获取加密处理后的运行数据并将所述加密处理后的运行数据发送至所述用户端。

[0034] 根据本发明的第二方面实施例的基于ARM架构的GPU可信执行系统，包括：

[0035] 基于ARM架构的可信固件，用于获取驱动端输出的安全程序执行信号；根据所述安全程序执行信号配置安全空间地址；根据所述安全空间地址，获取预存储在安全空间内的安全程序；对所述安全程序进行处理，生成认证GPU程序和解密数据；配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至所述用户端。

[0036] GPU，所述GPU连接所述基于ARM架构的可信固件，所述GPU用于根据所述认证 GPU程序和所述解密数据，生成运行数据；

[0037] 根据本发明实施例的基于ARM架构的GPU可信执行系统，至少具有如下有益效果：基于ARM架构的可信固件通过与驱动端和GPU之间的通信交互，可以获取驱动端输出的安全程序执行信号，并根据安全程序执行信号配置安全空间地址；根据安全空间地址，基于 ARM架构的可信固件可以获取预存储在安全空间内的安全程序，并对安全程序进行处理，生成认证GPU程序和解密数据。基于ARM架构的可信固件还能够获取并对安全空间与非安全空间之间的地址映射关系进行配置，以将加密输出的运行数据通过驱动端发送至用户端。GPU获取认证GPU程序和解密数据并执行认证GPU程序，并根据解密数据和认证 GPU程序的执行结果生成并输出运行数据，实现了将安全空间内的安全程序通过可信执行技术执行，并将在

可信环境下的产生的加密的运行数据从安全空间输出至非安全空间，实现了在基于ARM架构的设备中完成安全程序的可信执行，提高了GPU可信执行技术的兼容性和运行安全性。

[0038] 根据本发明的第三方面实施例的基于ARM架构的GPU可信执行设备，包括：

[0039] 至少一个处理器，以及

[0040] 与所述至少一个处理器通信连接的存储器，其中，

[0041] 所述存储器存储有指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器执行所述指令时实现如本发明第一方面实施例所述的基于ARM架构的GPU可信执行方法，

[0042] 根据本发明实施例的基于ARM架构的GPU可信执行设备，至少具有如下有益效果：本发明提供的基于ARM架构的GPU可信执行设备，通过执行如本发明第一方面实施例的基于ARM架构的GPU可信执行方法，通过获取安全程序执行信号为安全程序配置安全空间，并通过读取安全空间对应的安全空间地址，获取存储在安全空间内的安全程序；并通过对安全程序进行处理，获取认证的GPU程序和解密数据。根据认证GPU程序和解密数据，生成运行数据，并对安全空间地址进行释放，以使加密处理后的运行数据可以被释放到非安全空间，从而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储和安全运行，从而实现了在基于ARM架构的设备中完成安全程序的可信执行，提高了GPU可信执行技术的兼容性和运行安全性。

[0043] 根据本发明的第四方面实施例的计算机可读存储介质，包括：

[0044] 所述计算机可读存储介质存储有计算机可执行指令，可用于执行如本发明第一方面实施例所述的基于ARM架构的GPU可信执行方法。

[0045] 根据本发明实施例的计算机可读存储介质，至少具有如下有益效果：这种计算机可读存储介质存储有可执行指令，并通过执行基于ARM架构的GPU可信执行方法，能够获取安全程序执行信号为安全程序配置安全空间，并通过读取安全空间对应的安全空间地址，获取存储在安全空间内的安全程序。通过对安全程序进行处理，获取认证的GPU程序和解密数据。根据认证GPU程序和解密数据，生成运行数据，并对安全空间地址进行释放，以使加密处理后的运行数据可以被释放到非安全空间，从而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储和安全运行，从而实现了在基于ARM架构的设备中完成安全程序的可信执行，提高了GPU可信执行技术的兼容性和运行安全性。

[0046] 本发明的附加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

[0047] 下面结合附图和实施例对本发明做进一步的说明，其中：

[0048] 图1为本发明实施例基于ARM架构的GPU可信执行方法的流程图。

[0049] 图2为本发明实施例基于ARM架构的GPU可信执行方法的又一流程图。

[0050] 图3为本发明实施例基于ARM架构的GPU可信执行方法的又一流程图。

[0051] 图4为图1中步骤S400的流程图。

[0052] 图5为本发明实施例基于ARM架构的GPU可信执行方法的又一流程图。

[0053] 图6为图1中步骤S600的流程图。

[0054] 图7为本发明实施例基于ARM架构的GPU可信执行系统的结构示意图。

[0055] 附图标记:100,基于ARM架构的可信固件;200,GPU。

具体实施方式

[0056] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能理解为对本发明的限制。

[0057] 在本发明的描述中,需要理解的是,涉及到方位描述,例如上、下、前、后、左、右等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。

[0058] 在本发明的描述中,若干的含义是一个以上,多个的含义是两个以上,大于、小于、超过等理解为不包括本数,以上、以下、以内等理解为包括本数。如果有描述到第一、第二只是用于区分技术特征为目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量或者隐含指明所指示的技术特征的先后关系。

[0059] 本发明的描述中,除非另有明确的限定,设置、安装、连接等词语应做广义理解,所属技术领域技术人员可以结合技术方案的具体内容合理确定上述词语在本发明中的具体含义。

[0060] 本发明的描述中,参考术语“一个实施例”、“一些实施例”、“示意性实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0061] 第一方面,参照图1,本发明实施例提供了一种基于ARM架构的GPU可信执行方法,包括:

[0062] S100,获取驱动端输出的安全程序执行信号;

[0063] S200,根据安全程序执行信号配置安全空间地址;

[0064] S300,根据安全空间地址,获取预存储在安全空间内的安全程序;

[0065] S400,对安全程序进行处理,生成认证GPU程序和解密数据;

[0066] S500,根据认证GPU程序和解密数据,生成加密处理后的运行数据;

[0067] S600,配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至用户端。

[0068] 在本发明提供的基于ARM架构的GPU可信执行方法中,首先获取安全程序执行信号,为安全程序配置安全空间。通过读取安全空间对应的安全空间地址,获取存储在安全空间内的安全程序。通过对安全程序进行处理以获取认证的GPU程序和解密数据。根据获取到的认证GPU程序和解密数据,生成运行数据,并对安全空间地址进行释放,从而以使加密处理后的运行数据可以被释放到非安全空间,进而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储和安全运行,从而实现了在基于ARM架构的设备中完成安全程序的可信执行,提高了GPU可信执行技术的兼容性和运行安全性。

[0069] 在一些具体的实施例中，对于步骤S100和步骤S200，安全程序执行信号由驱动端发出。驱动端可以读取当前正在运行的GPU程序队列，并等待GPU中已有的程序运行结束，当获取到GPU中已有的程序运行结束时，将除安全程序中所包含的GPU任务以外的程序全部置于等待队列，并产生安全程序执行信号。当基于ARM的可信固件获取到安全程序执行信号时，通过配置安全空间地址来确定非安全空间与安全空间，隔绝非安全空间的进程或指令等对安全空间进行访问，并读取存储在安全空间的安全程序以进行运行安全程序的操作。本发明的一些实施例中，配置安全空间地址的方法可以是通过配置TrustZone地址空间控制器和地址转换表实现地址映射，但不限于此。

[0070] 参照图2，在一些实施例中，在步骤S100之前，该方法包括：

[0071] S710，通过用户端获取用户数据和GPU程序；

[0072] S720，用户端根据用户数据和GPU程序，生成安全程序；

[0073] S730，将安全程序存储至安全空间。

[0074] 本发明提供的基于ARM架构的GPU可信执行方法，可以在对获取到的用户信息进行加密生成用户数据，并存储用户数据和读取到的GPU程序。当GPU程序和用户数据被调用时，本方法可以控制用户端根据GPU程序和用户数据生成安全程序，并生成安全空间分配请求，以获取安全空间地址，使得安全程序可以被存储在安全空间内。这一方式实现了安全任务与非安全任务之间存储区域的分离，当运行安全任务对应的安全程序时，所需的数据均存储在安全空间内，能够避免非安全空间由于非法攻击导致的数据泄露，提高了方法安全性。

[0075] 参照图3，在一些实施例中，在步骤S100之前，还包括：

[0076] S810，通过GPU输出当前任务结束信号至驱动端；

[0077] S820，接收驱动端根据当前任务结束信号输出的安全程序执行信号。

[0078] 在本发明提供的基于ARM架构的GPU可信执行方法中，通过控制驱动端接收GPU输出的当前任务结束信号，可以先控制驱动端将除安全程序以外的其它待执行程序置于等待序列，再输出安全程序执行信号，使得当前GPU仅执行安全程序，也保证了安全程序运行过程中的独占性，提高了运行安全性。

[0079] 参照图4，在一些实施例中，步骤S400包括：

[0080] S410，根据安全程序，得到对应的用户数据和GPU程序；

[0081] S420，根据对GPU程序的完整性检验，生成认证GPU程序；

[0082] S430，根据获取到的解密算法对用户数据进行解密处理，生成解密数据。

[0083] 通过获取安全程序并对其进行解析，可以获取安全程序中的用户数据和GPU程序。通过检验GPU程序的完整性，生成认证GPU程序，并通过与用户端进行通信交互获取到的解密算法和密钥文件，对用户数据进行处理，可以获取解密数据。这一方式实现了对安全程序的安全性检验，提高了本发明中所提供的基于ARM架构的GPU可信执行方法的可靠性，也提高了执行过程的安全性，避免了由于传输错误或非法攻击导致安全程序内容异常导致的系统风险。

[0084] 在一些具体的实施例中，检验GPU程序的完整性，可以是通过哈希值检验的方法检验 GPU程序的完整性；通过与用户端进行通信交互获取到的解密算法和密钥文件，对用户数据进行处理。需要说明的是，获取解密数据中采取的解密算法可以是AES算法，但并不限于此。

[0085] 在一些实施例中，步骤S500之后，还包括：

[0086] 根据运行数据，生成安全程序结束信号

[0087] 当GPU运行安全程序结束后并生成运行数据时，通过本发明提供的基于ARM架构的GPU可信执行方法，可以控制GPU生成一个安全程序结束信号，以使GPU输出加密处理后的运行数据，进而执行步骤S500，以实现在ARM架构下的GPU可信执行技术，提高运行安全性。其中，安全程序结束信号可以是一种能被中断处理器获取到的中断信号，也可以是其它，不限于此。

[0088] 参照图5，在一些实施例中，步骤S600之前，该方法包括：

[0089] S910，根据安全程序结束信号，得到加密算法；

[0090] S920，根据加密算法对运行数据进行加密处理，生成加密处理后的运行数据。

[0091] 通过获取到的安全程序结束信号，本方法控制GPU与用户端进行通信交互获取加密算法，并根据加密算法对运行数据进行加密处理，生成加密处理后的运行数据。通过对运行数据的加密处理，可以进一步提高运行数据在传输过程中的安全性，保障本发明所提供的基于 ARM架构的GPU可信执行技术运行的安全性。

[0092] 参照图6，在一些实施例中，步骤S600包括：

[0093] S610，获取加密处理后的运行数据，并根据加密处理后的运行数据，配置安全空间与非安全空间的地址映射关系；

[0094] S620，根据地址映射关系，调取安全空间内的加密处理后的运行数据至非安全空间以使驱动端获取加密处理后的运行数据并将加密处理后的运行数据发送至用户端。

[0095] 本发明通过获取加密处理后的运行数据，控制基于ARM架构的可信固件配置安全空间与非安全空间之间的地址映射关系，使得加密处理后的运行数据可以通过重新配置后的地址映射关系从安全空间释放到非安全空间。通过获取安全程序结束信号，本方法控制驱动端从配置后的非安全空间获取到加密处理后的运行数据，并将加密处理后的运行数据转发至用户端，实现了安全程序在基于ARM架构的GPU的可信执行，也实现了在ARM架构下的GPU 可信执行技术，提高了运行安全性。

[0096] 在一些具体的实施例中，基于ARM架构的可信固件在接收到来自GPU输出的加密处理后的运行数据后，对S100中配置的安全空间地址再次采取通过配置TrustZone地址空间控制器和地址转换表来配置其地址映射，将加密处理后的运行数据从安全空间释放至非安全空间，以实现驱动端对加密处理后的运行数据的读取与转发至用户端的操作。

[0097] 第二方面，参照图7，本发明提供了一种基于ARM架构的GPU可信执行系统，包括基于ARM架构的可信固件100和GPU200，基于ARM架构的可信固件100用于获取驱动端输出的安全程序执行信号，根据安全程序执行信号配置安全空间地址，根据安全空间地址，获取预存储在安全空间内的安全程序；基于ARM架构的可信固件100还用于对安全程序进行处理，生成认证GPU200程序和解密数据；GPU200连接基于ARM架构的可信固件， GPU200用于根据认证GPU200程序和解密数据，生成运行数据，并配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至用户端。

[0098] 基于ARM架构的可信固件100通过与驱动端和GPU200之间的通信交互，可以获取驱动端输出的安全程序执行信号，并根据安全程序执行信号配置安全空间地址；基于ARM架构的可信固件100根据安全空间地址，获取预存储在安全空间内的安全程序，并对安全程序进

行处理,生成认证GPU程序和解密数据;GPU200可以执行认证GPU程序,并根据解密数据和认证GPU程序的执行结果生成运行数据。基于ARM架构的可信固件100在获取到 GPU200输出的加密处理后的运行数据后,对安全空间与非安全空间之间的地址映射关系进行配置,以实现将加密输出的运行数据通过驱动端发送至用户端,这一方式实现了运行数据的加密和将安全空间内的安全程序通过可信执行技术执行,并将在可信环境下的产生的加密的运行数据从安全空间输出至非安全空间,实现了在基于ARM架构的设备中完成安全程序的可信执行,提高了运行安全性。

[0099] 第三方面,本发明提供了一种基于ARM架构的GPU可信执行设备,包括:

[0100] 至少一个处理器,以及

[0101] 与所述至少一个处理器通信连接的存储器,其中,

[0102] 所述存储器存储有指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器执行所述指令时实现如本发明第一方面实施例所述的基于ARM架构的GPU可信执行方法,

[0103] 根据本发明实施例的基于ARM架构的GPU可信执行设备,至少具有如下有益效果:本发明提供的基于ARM架构的GPU可信执行设备,通过执行如本发明第一方面实施例的基于ARM架构的GPU可信执行方法,能够获取安全程序执行信号,为安全程序配置安全空间。通过读取安全空间对应的安全空间地址,获取存储在安全空间的安全程序。通过对安全程序进行处理以获取认证的GPU程序和解密数据。根据获取到的认证GPU程序和解密数据,生成运行数据,并对安全空间地址进行释放,从而以使加密处理后的运行数据可以被释放到非安全空间,进而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储,和安全程序运行时可以独占GPU当前运行任务序列的技术手段,从而实现了在基于 ARM架构的设备中完成安全程序的可信执行,提高了GPU可信执行技术的兼容性和运行安全性。

[0104] 第四方面,本发明提供了一种计算机可读存储介质,计算机可读存储介质存储有计算机可执行指令,可用于执行如本发明第一方面实施例所述的基于ARM架构的GPU可信执行方法。

[0105] 通过采取本发明提供的计算机可读存储介质,可以通过执行计算机可读存储介质存储的可执行指令,能够获取安全程序执行信号为安全程序配置安全空间。并通过读取安全空间对应的安全空间地址,获取存储在安全空间的安全程序。通过对安全程序进行处理,获取认证的GPU程序和解密数据。根据认证GPU程序和解密数据,生成运行数据,并对安全空间地址进行释放,以使加密处理后的运行数据可以被释放到非安全空间,从而使用户端获取到加密后的运行数据。实现了对于安全程序的安全存储和安全运行,从而实现了在基于ARM架构的设备中完成安全程序的可信执行,提高了GPU可信执行技术的兼容性和运行安全性。

[0106] 上面结合附图对本发明实施例作了详细说明,但是本发明不限于上述实施例,在所属技术领域普通技术人员所具备的知识范围内,还可以在不脱离本发明宗旨的前提下作出各种变化。此外,在不冲突的情况下,本发明的实施例及实施例中的特征可以相互组合。

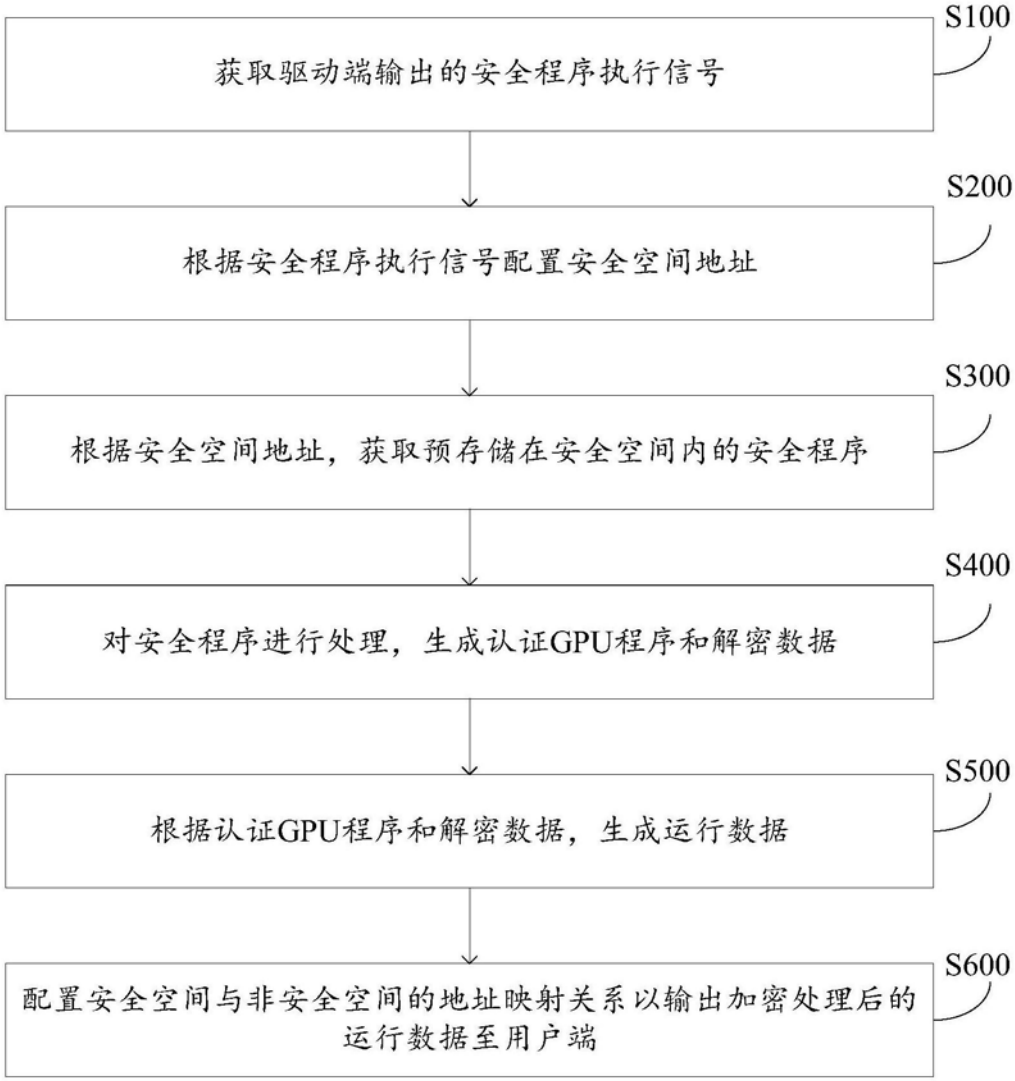

S100
获取驱动端输出的安全程序执行信号
S200
根据安全程序执行信号配置安全空间地址
S300
根据安全空间地址，获取预存储在安全空间内的安全程序
S400
对安全程序进行处理，生成认证GPU程序和解密数据
S500
根据认证GPU程序和解密数据，生成运行数据
S600
配置安全空间与非安全空间的地址映射关系以输出加密处理后的运行数据至用户端

图1

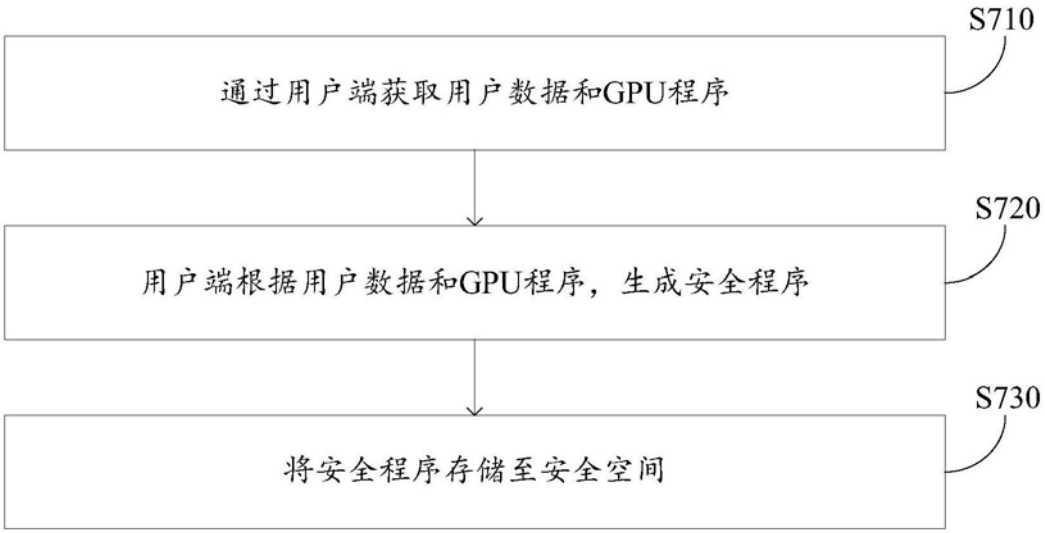

S710
通过用户端获取用户数据和GPU程序
S720
用户端根据用户数据和GPU程序，生成安全程序
S730
将安全程序存储至安全空间

图2

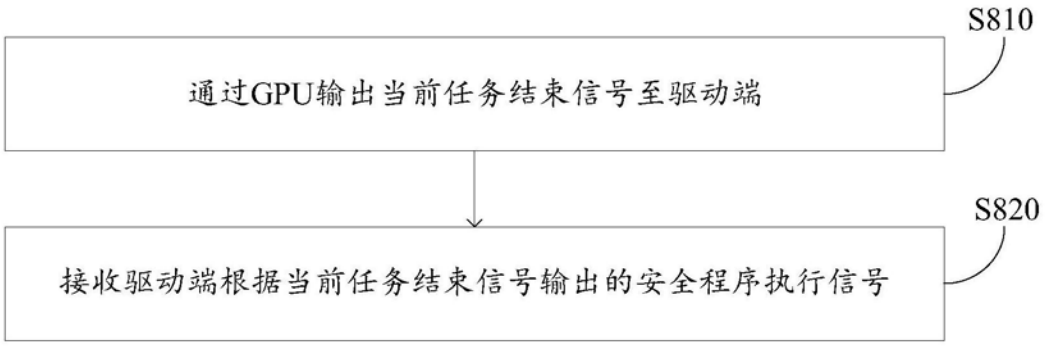

S810
通过GPU输出当前任务结束信号至驱动端
S820
接收驱动端根据当前任务结束信号输出的安全程序执行信号

图3

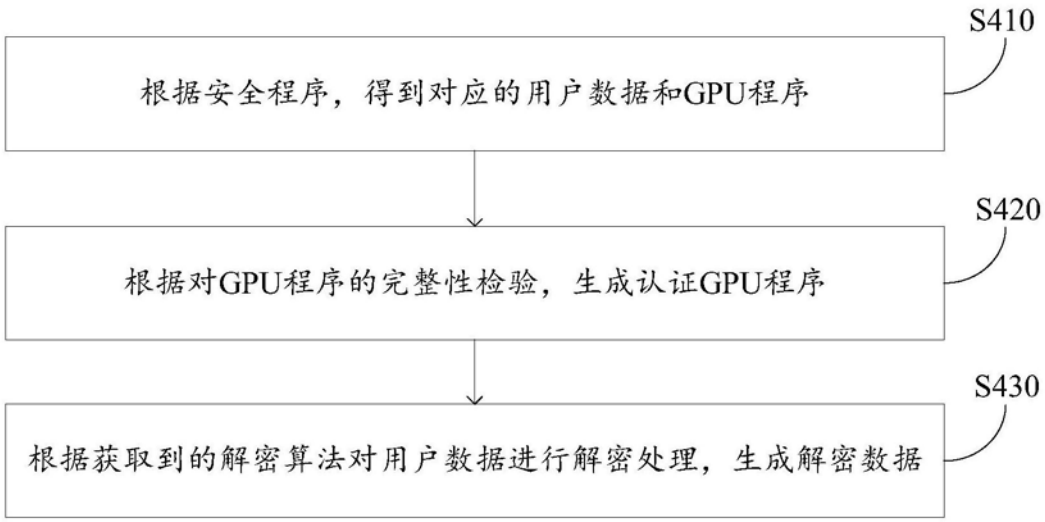

S410
根据安全程序，得到对应的用户数据和GPU程序
S420
根据对GPU程序的完整性检验，生成认证GPU程序
S430
根据获取到的解密算法对用户数据进行解密处理，生成解密数据

图4

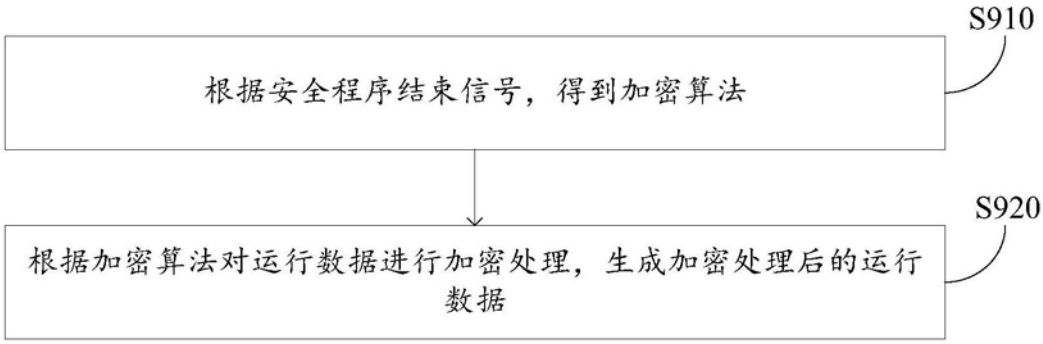

S910
根据安全程序结束信号，得到加密算法
S920
根据加密算法对运行数据进行加密处理，生成加密处理后的运行数据

图5

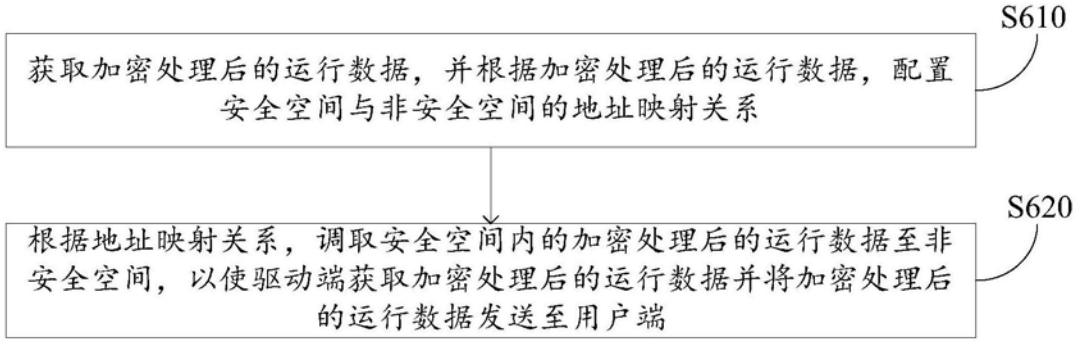

S610
获取加密处理后的运行数据，并根据加密处理后的运行数据，配置安全空间与非安全空间的地址映射关系
S620
根据地址映射关系，调取安全空间内的加密处理后的运行数据至非安全空间，以使驱动端获取加密处理后的运行数据并将加密处理后的运行数据发送至用户端

图6

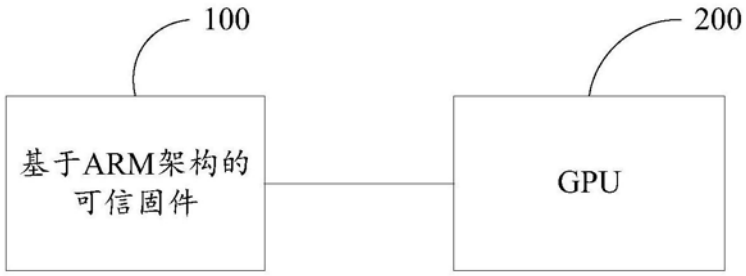

100
200
基于ARM架构的可信固件
GPU

图7