(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114553607 A
(43)申请公布日 2022.05.27

(21)申请号 202210441877.9

(22)申请日 2022.04.26

(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 周雷 张锋巍

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
专利代理师 洪铭福

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/12(2022.01)

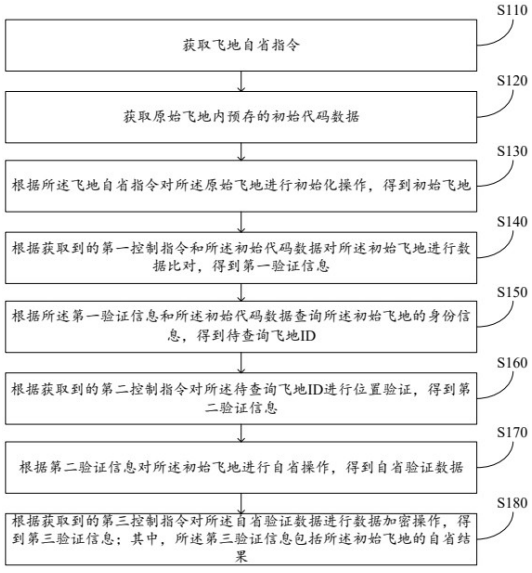
权利要求书3页 说明书12页 附图6页

(54)发明名称

飞地实时自省方法、飞地实时自省装置及电子设备

(57)摘要

本申请公开了一种飞地实时自省方法、飞地实时自省装置及电子设备。属于信息安全领域。本申请通过获取飞地自省指令;获取原始飞地内预存的初始代码数据;根据飞地自省指令对原始飞地进行初始化操作,得到初始飞地;根据获取到的第一控制指令和初始代码数据对初始飞地进行数据比对,得到第一验证信息;根据第一验证信息和初始代码数据查询初始飞地的身份信息,得到待查询飞地ID;根据获取到的第二控制指令对待查询飞地ID进行位置验证,得到第二验证信息;根据第二验证信息对初始飞地进行自省操作,得到自省验证数据;根据获取到的第三控制指令对自省验证数据进行数据加密操作,得到第三验证信息,进而提供了一种安全可靠的飞地实时自省方法。



CN 114553607 A

1.飞地实时自省方法,应用于第一线程,其特征在于,包括:

获取飞地自省指令;

获取原始飞地内预存的初始代码数据;

根据所述飞地自省指令对所述原始飞地进行初始化操作,得到初始飞地;

根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对,得到第一验证信息;

根据所述第一验证信息和所述初始代码数据查询所述初始飞地的身份信息,得到待查询飞地ID;

根据获取到的第二控制指令对所述待查询飞地ID进行位置验证,得到第二验证信息;

根据第二验证信息对所述初始飞地进行自省操作,得到自省验证数据;

根据获取到的第三控制指令对所述自省验证数据进行数据加密操作,得到第三验证信息;其中,所述第三验证信息包括所述初始飞地的自省结果。

2.根据权利要求1所述的飞地实时自省方法,其特征在于,在所述获取原始飞地内预存的初始代码数据之前,所述方法还包括:

获取锚代码数据和自省代码数据;

根据所述锚代码数据和所述自省代码数据生成所述初始代码数据;

根据所述原始飞地的通信地址,将所述初始代码数据存储至所述原始飞地。

3.根据权利要求1或2所述的飞地实时自省方法,其特征在于,所述根据所述飞地自省指令对所述原始飞地进行初始化操作,得到初始飞地,包括:

根据所述飞地自省指令获取预设的蹦床程序;

根据所述蹦床程序执行预设的初始化代码,对所述原始飞地的飞地页面缓存进行配置;

根据所述蹦床程序,更改所述原始飞地的默认处理程序,得到所述初始飞地。

4.根据权利要求2所述的飞地实时自省方法,其特征在于,所述初始代码数据包括锚代码数据,所述根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对,得到第一验证信息,包括:

实时获取所述第一控制指令,当获取到所述第一控制指令时,执行以下步骤:

获取所述初始飞地的状态保存页面内存数据和所述锚代码数据;

将所述状态保存页面内存数据和所述锚代码数据输出至预设的存储区域;

在所述存储区域内,控制所述初始飞地的代理程序根据所述锚代码数据对所述状态保存页面内存数据进行数据比对,并根据比对结果得到第一验证信息。

5.根据权利要求1所述的飞地实时自省方法,其特征在于,所述根据获取到的第二控制指令对所述待查询飞地ID进行位置验证,得到第二验证信息,包括:

实时获取所述第二控制指令,当获取到所述第二控制指令时,执行以下步骤:

控制所述初始飞地的代理程序获取预设的飞地原始ID;

将所述飞地原始ID与所述待查询飞地ID进行数据比对,得到所述第二验证信息。

6.根据权利要求1所述的飞地实时自省方法,其特征在于,所述根据获取到的第三控制指令对所述自省验证数据进行数据加密操作,得到第三验证信息,包括:

实时获取所述第三控制指令,当获取到所述第三控制指令时,执行以下步骤:

获取预设的加密密钥；

控制所述初始飞地的代理程序根据所述加密密钥对所述自省验证数据进行数据加密操作，得到所述第三验证信息。

7.飞地实时自省方法，应用于第二线程，其特征在于，包括：

根据预设的监控开始请求，检测共享内存的读写状态；其中所述共享内存存储有初始代码数据；

根据所述读写状态，实时获取飞地自省指令；

根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；

根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；

根据获取到的第二验证信息，输出第三控制指令。

8.飞地实时自省装置，应用于第一线程，其特征在于，包括：

指令获取模块，用于获取飞地自省指令；

代码获取模块，用于获取原始飞地内预存的初始代码数据；

初始化模块，用于根据所述飞地自省指令对所述原始飞地进行初始化操作，得到初始飞地；

第一验证模块，用于根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对，得到第一验证信息；

第一数据模块，用于根据所述第一验证信息和所述初始代码数据查询所述初始飞地的身份信息，得到待查询飞地ID；

第二验证模块，用于根据获取到的第二控制指令对所述待查询飞地ID进行位置验证，得到第二验证信息；

第二数据模块，用于根据第二验证信息对所述初始飞地进行自省操作，得到自省验证数据；

第三数据模块，用于根据获取到的第三控制指令对所述自省验证数据进行数据加密操作，得到第三验证信息；其中，所述第三验证信息包括所述初始飞地的自省结果。

9.飞地实时自省装置，应用于第二线程，其特征在于，包括：

检测模块，用于根据预设的监控开始请求，检测共享内存的读写状态；其中所述共享内存存储有初始代码数据；

指令生成模块，用于根据所述读写状态，实时获取飞地自省指令；

第一输出模块，用于根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；

第二输出模块，用于根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；

第三输出模块，用于根据获取到的第二验证信息，输出第三控制指令。

10.电子设备，其特征在于，包括：

至少一个存储器，以及

与所述至少一个存储器通信连接的处理器，其中；

所述至少一个存储器存储有计算机可执行指令，所述处理器用于执行所述计算机可执行指令，以使计算机执行所述计算机可执行指令时，实现如权利要求1至6任一项所述的飞

地实时自省方法,或者实现如权利要求7所述的飞地实时自省方法。

飞地实时自省方法、飞地实时自省装置及电子设备

技术领域

[0001] 本申请涉及信息安全领域，尤其是涉及一种飞地实时自省方法、飞地实时自省装置及电子设备。

背景技术

[0002] 相关技术中，代理程序通常采用SGX本地/远程证明机制对飞地的身份信息进行校验，从而根据飞地的自身代码获取验证报告。这一方法无法保证在远程通信的过程中不被攻击，从而无法保证飞地内存自省过程的安全性。因此，如何提供一种安全可靠的飞地实时自省方法，成为了一个亟待解决的问题。

发明内容

[0003] 本申请旨在至少解决现有技术中存在的技术问题之一。为此，本申请提出一种飞地实时自省方法，应用于第一线程，能够在不依赖于飞地本地/远程证明机制的前提下，通过对飞地的预处理实现飞地的实时自省。

[0004] 本申请还提出一种飞地实时自省方法，应用于第二线程。

[0005] 本申请还提出一种具有上述飞地实时自省方法的飞地实时自省装置。

[0006] 本申请还提出一种具有上述飞地实时自省方法的电子设备。

[0007] 根据本申请的第一方面实施例的飞地实时自省方法，应用于第一线程，包括：

获取飞地自省指令；

获取原始飞地内预存的初始代码数据；

根据所述飞地自省指令对所述原始飞地进行初始化操作，得到初始飞地；

根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对，得到第一验证信息；

根据所述第一验证信息和所述初始代码数据查询所述初始飞地的身份信息，得到待查询飞地ID；

根据获取到的第二控制指令对所述待查询飞地ID进行位置验证，得到第二验证信息；

根据第二验证信息对所述初始飞地进行自省操作，得到自省验证数据；

根据获取到的第三控制指令对所述自省验证数据进行数据加密操作，得到第三验证信息；其中，所述第三验证信息包括所述初始飞地的自省结果。

[0008] 根据本申请第一方面实施例的飞地实时自省方法，至少具有如下有益效果：

本申请提供的应用于第一线程的飞地实时自省方法，可以获取飞地自省指令，其中飞地自省指令由代理程序发出，用于触发飞地的自省；还可以获取初始飞地内存储的初始代码数据；通过飞地自省指令，本方法可以对原始飞地进行初始化操作，得到初始飞地，并根据初始代码数据和获取到的第一控制指令对对初始飞地内的初始代码数据的数据合法性进行数据比对，得到第一验证信息；通过第一验证信息和初始代码数据，本方法可以定

位到需要查询的飞地对应的ID,得到待查询飞地ID,并根据获取到的第二控制指令对待查询飞地ID的身份信息合法性进行位置验证,得到包含验证通过信息的第二验证信息;通过第二验证信息,本方法进一步的对初始飞地的内存进行自省进而对初始飞地的身份合法性进行查询,得到自省验证数据;通过获取到的第三控制指令,本方法可以将自省验证数据进行数据加密,得到的第三验证信息,以进一步的将加密后的第三验证信息输出至代理程序。本申请提供的飞地实时自省方法可以通过对原始飞地进行初始化操作以更改飞地内数据的调用权限,校验初始代码数据的存储状态并通过飞地内预存的初始代码数据对初始飞地的身份信息进行查询,从而根据包含初始飞地身份信息的飞地ID对飞地进行检测,进而检测初始飞地的可信性,以对位置检测的初始飞地实现自省操作。本方法有效的实现了对初始飞地的自省,并通过对自行得到的自省验证数据加密得到第三验证信息,使得用户可以通过代理程序实时获取当前初始飞地的自省结果,避免了基于SGX本地/远程机制对飞地进行自省时,无法保证通信过程的安全性以及无法阻止非法攻击的风险,提供了一种更为安全的飞地实时自省方法。

[0009] 根据本申请的一些实施例,在所述获取原始飞地内预存的初始代码数据之前,所述方法还包括:

获取锚代码数据和自省代码数据;

根据所述锚代码数据和所述自省代码数据生成所述初始代码数据;

根据所述原始飞地的通信地址,将所述初始代码数据存储至所述原始飞地。

[0010] 根据本申请的一些实施例,所述根据所述飞地自省指令对所述原始飞地进行初始化操作,得到初始飞地,包括:

根据所述飞地自省指令获取预设的蹦床程序;

根据所述蹦床程序执行预设的初始化代码,对所述原始飞地的飞地页面缓存进行配置;

根据所述蹦床程序,更改所述原始飞地的默认处理程序,得到所述初始飞地。

[0011] 根据本申请的一些实施例,所述初始代码数据包括锚代码数据,所述根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对,得到第一验证信息,包括:

实时获取所述第一控制指令,当获取到所述第一控制指令时,执行以下步骤:

获取所述初始飞地的状态保存页面内存数据和所述锚代码数据;

将所述状态保存页面内存数据和所述锚代码数据输出至预设的存储区域;

在所述存储区域内,控制所述初始飞地的代理程序根据所述锚代码数据对所述状态保存页面内存数据进行数据比对,并根据比对结果得到第一验证信息。

[0012] 根据本申请的一些实施例,所述根据获取到的第二控制指令对所述待查询飞地ID进行位置验证,得到第二验证信息,包括:

实时获取所述第二控制指令,当获取到所述第二控制指令时,执行以下步骤:

控制所述初始飞地的代理程序获取预设的飞地原始ID;

将所述飞地原始ID与所述待查询飞地ID进行数据比对,得到所述第二验证信息。

[0013] 根据本申请的一些实施例,所述根据获取到的第三控制指令对所述自省验证数据进行数据加密操作,得到第三验证信息,包括:

实时获取所述第三控制指令，当获取到所述第三控制指令时，执行以下步骤：

获取预设的加密密钥；

控制所述初始飞地的代理程序根据所述加密密钥对所述自省验证数据进行数据加密操作，得到所述第三验证信息。

[0014] 根据本申请的第二方面实施例的飞地实时自省方法，应用于第二线程，包括：

根据预设的监控开始请求，检测共享内存的读写状态；其中所述共享内存存储有初始代码数据；

根据所述读写状态，实时获取飞地自省指令；

根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；

根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；

根据获取到的第二验证信息，输出第三控制指令。

[0015] 根据本申请第二方面实施例的飞地实时自省方法，至少具有如下有益效果：

本申请所提供的飞地实时自省方法，可以应用于第二线程，以使第二线程根据共享内存的读写状态和第一线程输出的验证信息输出对应的控制指令，以使第一线程可以控制指令对飞地进行实时自省。具体地，本方法可以根据预设的监控开始请求控制第二线程监控共享内存的读写状态。其中，共享内存存储有初始代码数据。并在检测到共享内存的读写状态为正在读写时，实时获取第一线程获取到的飞地自省指令，从而根据飞地自省指令输出第一控制指令，以控制第一线程根据第一控制指令输出第一验证信息，从而使第二线程通过实时监控第一验证信息获取第一验证信息；根据第一验证信息，本方法控制第二线程输出第二控制指令至第一线程，以使第一线程根据第二控制指令输出第二验证信息，从而使第二线程通过实时监控第二验证信息获取第二验证信息；通过第二验证信息，本方法可以控制第二线程将第三控制指令输出至第一线程，以使第一线程根据第三控制指令实现对自省验证数据的加密操作。通过这一方法，本申请可以有效的对共享内存内初始代码数据的调用状态进行监控，当监控到初始代码数据被第一线程调用时，可以根据第一线程的执行状态输出不同的控制指令，以协助第一线程根据第二线程输出的第一控制指令或者第二控制指令或者第三控制指令执行相应的操作，从而实现对飞地的实时自省以及自省结果的加密。

[0016] 根据本申请的第三方面实施例的飞地实时自省装置，应用于第一线程，包括：

指令获取模块，用于获取飞地自省指令；

代码获取模块，用于获取原始飞地内预存的初始代码数据；

初始化模块，用于根据所述飞地自省指令对所述原始飞地进行初始化操作，得到初始飞地；

第一验证模块，用于根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对，得到第一验证信息；

第一数据模块，用于根据所述第一验证信息和所述初始代码数据查询所述初始飞地的身份信息，得到待查询飞地ID；

第二验证模块，用于根据获取到的第二控制指令对所述待查询飞地ID进行位置验证，得到第二验证信息；

第二数据模块，用于根据第二验证信息对所述初始飞地进行自省操作，得到自省

验证数据；

第三数据模块，用于根据获取到的第三控制指令对所述自省验证数据进行数据加密操作，得到第三验证信息；其中，所述第三验证信息包括所述初始飞地的自省结果。

[0017] 根据本申请第三方面实施例的飞地实时自省装置，应用于第一线程，至少具有如下有益效果：

根据本申请实施例应用于第一线程的飞地实时自省装置，通过指令获取模块可以获取飞地自省指令，并将飞地自省指令输出至代码获取模块以获取初始飞地内预存的初始代码数据；通过初始化模块，本申请可以根据飞地自省指令对原始飞地进行初始化操作，从而生成初始飞地；通过第一验证模块，本申请可以根据获取到的第一控制指令和初始代码数据对初始飞地进行数据比对，得到第一验证信息；第一数据模块，用于根据第一验证信息和初始代码数据查询初始飞地的身份信息，得到待查询飞地ID；通过第二验证模块，本装置可以获取到的第二控制指令对待查询飞地ID进行位置验证，得到第二验证信息；通过第二数据模块，本装置可以根据第二验证信息对初始飞地进行自省操作，得到自省验证数据；通过第三数据模块，本装置可以根据获取到的第三控制指令对自省验证数据进行数据加密操作，得到第三验证信息；其中，第三验证信息包括初始飞地的自省结果。通过本发明提供的应用于第一线程的飞地实时自省装置，本申请可以通过对原始飞地进行初始化操作以更改飞地内数据的调用权限，校验初始代码数据的存储状态并通过飞地内预存的初始代码数据对初始飞地的身份信息进行查询，从而根据包含初始飞地身份信息的飞地ID对飞地进行检测，进而检测初始飞地的可信性，以对位置检测的初始飞地实现自省操作。本装置有效的实现了对初始飞地的自省，并通过对自行得到的自省验证数据加密得到第三验证信息，使得用户可以通过代理程序实时获取当前初始飞地的自省结果，避免了基于SGX本地/远程机制对飞地进行自省时，无法保证通信过程的安全性以及无法阻止非法攻击的风险，提供了一种更为安全的飞地实时自省装置。

[0018] 根据本申请的第四方面实施例的飞地实时自省装置，应用于第二线程，包括：

检测模块，用于根据预设的监控开始请求，检测共享内存的读写状态；其中所述共享内存存储有初始代码数据；

指令生成模块，用于根据所述读写状态，实时获取飞地自省指令；

第一输出模块，用于根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；

第二输出模块，用于根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；

第三输出模块，用于根据获取到的第二验证信息，输出第三控制指令。

[0019] 根据本申请第四方面实施例的飞地实时自省装置，应用于第二线程，至少具有如下有益效果：

根据本申请实施例应用于第一线程的飞地实时自省装置，本申请可以通过检测模块实现根据预设的监控开始请求，检测共享内存的读写状态；其中共享内存存储有初始代码数据；通过指令生成模块，本申请可以根据读写状态，实时获取飞地自省指令；通过第一输出模块，本申请可以根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；通过第二输出模块，本申请可以根据获取到的第一验证信息，输出第二控制指令，

并实时获取第二验证信息;通过第三输出模块,本申请可以根据获取到的第二验证信息,输出第三控制指令。通过本申请提供的应用于第二线程的飞地实时自省装置,本发明可以使第二线程根据共享内存的读写状态和第一线程输出的验证信息输出对应的控制指令,以使第一线程可以控制指令对飞地进行实时自省。具体地,本装置可以根据预设的监控开始请求控制第二线程监控共享内存的读写状态。其中,共享内存存储有初始代码数据。并在检测到共享内存的读写状态为正在读写时,实时获取第一线程获取到的飞地自省指令,从而根据飞地自省指令输出第一控制指令,以控制第一线程根据第一控制指令输出第一验证信息,从而使第二线程通过实时监控第一验证信息获取第一验证信息;根据第一验证信息,本装置控制第二线程输出第二控制指令至第一线程,以使第一线程根据第二控制指令输出第二验证信息,从而使第二线程通过实时监控第二验证信息获取第二验证信息;通过第二验证信息,本装置可以控制第二线程将第三控制指令输出至第一线程,以使第一线程根据第三控制指令实现对自省验证数据的加密操作。通过这一装置,本申请可以有效的对共享内存内初始代码数据的调用状态进行监控,当监控到初始代码数据被第一线程调用时,可以根据第一线程的执行状态输出不同的控制指令,以协助第一线程根据第二线程输出的第一控制指令或者第二控制指令或者第三控制指令执行相应的操作,从而实现对飞地的实时自省以及自省结果的加密。

[0020] 根据本申请的第五方面实施例的电子设备,包括:

至少一个存储器,以及

与所述至少一个存储器通信连接的处理器,其中;

所述至少一个存储器存储有计算机可执行指令,所述处理器用于执行所述计算机可执行指令,以使计算机执行所述计算机可执行指令时,实现如本发明第一方面实施例所述的飞地实时自省方法,或者实现如本发明第二方面实施例所述的飞地实时自省方法。

[0021] 本申请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,或通过本申请的实践了解到。

附图说明

[0022] 下面结合附图和实施例对本申请做进一步的说明,其中:

图1为本申请实施例的飞地实时自省方法的流程图;

图2为图1中步骤S120之前的流程图;

图3为图1中步骤S130的具体流程图;

图4为图1中步骤S140的具体流程图;

图5为图1中步骤S160的具体流程图;

图6为图1中步骤S180的具体流程图;

图7为本申请实施例的飞地实时自省方法的又一流程图;

图8为本申请实施例的飞地实时自省装置的结构图;

图9为本申请实施例的飞地实时自省装置的又一结构图;

附图标记:指令获取模块810;初始化模块820;代码获取模块830;第一验证模块840;第一数据模块850;第二验证模块860;第二数据模块870;第三数据模块880;检测模块910;指令生成模块920;第一输出模块930;第二输出模块940;第三输出模块950。

具体实施方式

[0023] 下面详细描述本申请的实施例，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，仅用于解释本申请，而不能理解为对本申请的限制。

[0024] 在本申请的描述中，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申请和简化描述，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申请的限制。

[0025] 在本申请的描述中，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。

[0026] 本申请的描述中，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申请中的具体含义。

[0027] 本申请的描述中，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申请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。

[0028] 第一方面，参照图1，本发明提供了一种飞地实时自省方法，应用于第一线程，包括：

步骤S110，获取飞地自省指令；

步骤S120，获取原始飞地内预存的初始代码数据；

步骤S130，根据飞地自省指令对原始飞地进行初始化操作，得到初始飞地；

步骤S140，根据获取到的第一控制指令和初始代码数据对初始飞地进行数据比对，得到第一验证信息；

步骤S150，根据第一验证信息和初始代码数据查询初始飞地的身份信息，得到待查询飞地ID；

步骤S160，根据获取到的第二控制指令对待查询飞地ID进行位置验证，得到第二验证信息；

步骤S170，根据第二验证信息对初始飞地进行自省操作，得到自省验证数据；

步骤S180，根据获取到的第三控制指令对自省验证数据进行数据加密操作，得到第三验证信息；其中，第三验证信息包括初始飞地的自省结果。

[0029] 本申请提供的应用于第一线程的飞地实时自省方法，可以获取飞地自省指令，其中飞地自省指令由代理程序发出，用于触发飞地的自省；还可以获取初始飞地内存储的初始代码数据；通过飞地自省指令，本方法可以对原始飞地进行初始化操作，得到初始飞地，并根据初始代码数据和获取到的第一控制指令对对初始飞地内的初始代码数据的数据合法性进行数据比对，得到第一验证信息；通过第一验证信息和初始代码数据，本方法可以定

位到需要查询的飞地对应的ID,得到待查询飞地ID,并根据获取到的第二控制指令对待查询飞地ID的身份信息合法性进行位置验证,得到包含验证通过信息的第二验证信息;通过第二验证信息,本方法进一步的对初始飞地的内存进行自省进而对初始飞地的身份合法性进行查询,得到自省验证数据;通过获取到的第三控制指令,本方法可以将自省验证数据进行数据加密,得到的第三验证信息,以进一步的将加密后的第三验证信息输出至代理程序。本申请提供的飞地实时自省方法可以通过对原始飞地进行初始化操作以更改飞地内数据的调用权限,校验初始代码数据的存储状态并通过飞地内预存的初始代码数据对初始飞地的身份信息进行查询,从而根据包含初始飞地身份信息的飞地ID对飞地进行检测,进而检测初始飞地的可信性,以对位置检测的初始飞地实现自省操作。本方法有效的实现了对初始飞地的自省,并通过对自行得到的自省验证数据加密得到第三验证信息,使得用户可以通过代理程序实时获取当前初始飞地的自省结果,避免了基于SGX本地/远程机制对飞地进行自省时,无法保证通信过程的安全性以及无法阻止非法攻击的风险,提供了一种更为安全的飞地实时自省方法。

[0030] 参照图2,在一些实施例中,步骤S130之前,飞地实时自省方法还包括:

步骤S210,获取锚代码数据和自省代码数据;

步骤S220,根据锚代码数据和自省代码数据生成初始代码数据;

步骤S230,根据原始飞地的通信地址,将初始代码数据存储至原始飞地。

[0031] 本申请所提供的飞地实时自省方法在获取初始飞地内预存的初始代码之前,还会根据锚代码数据和自省代码数据生成初始代码数据,并将初始代码数据预存至初始飞地。首先,先对锚代码数据和自省代码数据进行解释。

[0032] 执行本申请提供的锚代码数据,本方法可以控制初始飞地输出初始飞地内状态保存页面的内存数据,并将内存数据转存至预设的存储空间。随后,执行锚代码数据,本方法可以输出用于自省的自省代码页面数据,并控制初始飞地跳转至自省代码数据。需要注意的是,预设的存储空间为共享内存,且为非飞地缓存页面,这一预设的存储空间用于存储内存数据,同时也可以与第二线程进行共享,使得第二线程对这一存储空间进行共享时,对存储空间内存储的初始代码数据进行查询。

[0033] 执行本申请提供的自省代码数据,本方法可以使用户用于与初始飞地进行指令交互的代理程序获取初始飞地的身份信息,并通过代理程序对初始飞地的身份信息进行验证,从而对通过验证的初始飞地进行自省,以实时验证初始飞地的安全性。

[0034] 本申请所提供的飞地实时自省方法,通过获取预设的锚代码数据和自省代码数据,可以得到初始代码数据,并将初始代码数据存储至初始飞地中,使得与初始飞地进行通信交互的代理程序可以根据上述执行步骤对初始飞地的身份信息进行校验,并对初始飞地进行自省,进而实现本申请提供的飞地实时自省方法。

[0035] 在一些具体的实施例中,锚代码数据仅包含十行指令,通过第一至第三行指令,本方法可以输出初始飞地的状态保存页面内的内存数据;通过第四至第六行指令,本方法可以输出预设的锚代码数据对应的页面数据至预设的存储空间,锚代码数据对应的页面数据由控制指令以及随机字节完全填充,以避免外来数据攻击对初始飞地造成干扰;通过第六至第十行指令,本方法可以控制初始飞地输出自省代码数据,并跳转至执行自省代码数据部分的程序。

[0036] 参照图3,在一些实施例中,步骤S120包括:

步骤S310,根据飞地自省指令获取预设的蹦床程序;

步骤S320,根据蹦床程序执行预设的初始化代码,对原始飞地的飞地页面缓存进行配置;

步骤S330,根据蹦床程序,更改原始飞地的默认处理程序,得到初始飞地。

[0037] 本申请提供的飞地实时自省方法可以通过飞地自省指令获取预设的蹦床程序,并通过蹦床程序执行预设的初始化代码,对原始飞地的飞地页面缓存进行配置,从而使原始飞地中的访问机制被拦截,使得任何对经过配置后的原始飞地的访问仅能通过蹦床程序对原始飞地内进行修改,进而使得蹦床程序成为新的默认程序,以得到初始飞地。通过这一方法,本申请可以避免外部对初始飞地的内核访问,从而保证飞地自省过程中的安全性。

[0038] 在一些具体的实施例中,蹦床程序通过配置飞地中各类内存页面实现对原始飞地的初始化,即实现对原始飞地内存访问权限的修改。具体地,本方法可以控制蹦床程序将原始飞地的锚代码数据的配置页面和状态保存页面修改为可访问状态,并将全部的飞地缓存页面的访问权限修改为不可访问状态,并通过删除原始飞地内包含原访问映射关系的内存页表内的指针数据,防止外部指令对经过初始化处理后得到的初始飞地的内核,从而保证初始飞地的安全性。

[0039] 参照图4,在一些实施例中,初始代码数据包括锚代码数据,步骤S140包括:

步骤S410,实时获取第一控制指令,当获取到第一控制指令时,执行以下步骤:

步骤S420,获取初始飞地的状态保存页面内存数据和锚代码数据;

步骤S430,将状态保存页面内存数据和锚代码数据输出至预设的存储区域;

步骤S440,在存储区域内,控制初始飞地的代理程序根据锚代码数据对状态保存页面内存数据进行数据比对,并根据比对结果得到第一验证信息。

[0040] 本申请所提供的飞地实时自省方法通过实时获取到的第一控制指令,对初始飞地的状态保存页面内存数据和锚代码数据进行获取,并将状态保存页面内存数据和锚代码数据输出至预设的存储区域,以使代理程序对状态保存页面内存数据和锚数据进行比对,进而实时同步初始飞地和代理程序之间的处理进度,当本方法完成初始飞地和代理程序之间的进度同步时,输出第一验证信息。通过这一方法,本申请可以将与初始飞地通信连接的代理程序与初始飞地的工作状态保持一致,从而实现后续对初始飞地的实时自省。

[0041] 在一些具体的实施例中,当获取到第一控制指令时,蹦床程序会将状态保存页面内存数据和锚代码数据输出至预设的存储区域,这一存储区域为共享内存,共享内存内存储有对应的同步标识符,识别同步标识符,本方法可以控制蹦床程序同步初始飞地与代理程序之间的工作状态,并在工作状态完成同步之后输出第一验证信息,以使蹦床程序进一步根据第一验证信息将共享内存内的工作代码数据输出至非飞地缓存页面中,并跳转至自省代码数据部分,实现对工作代码数据的自省过程,从而实现对初始飞地的实时自省。在一些其他的实施例中,本方法提供了一个不可写代码页和三个可写代码页作为非飞地缓存页面,不可写代码页中存储有enter指令,并用0对不可写代码页中其余空间进行填充。三个可写代码页用于存储初始飞地根据各种指令输出的数据。

[0042] 参照图5,在一些实施例中,步骤S160包括:

步骤S510,实时获取第二控制指令,当获取到第二控制指令时,执行以下步骤:

步骤S520,控制初始飞地的代理程序获取预设的飞地原始ID;

步骤S530,将飞地原始ID与待查询飞地ID进行数据比对,得到第二验证信息。

[0043] 本申请所提供的飞地实时自省方法通过实时获取到的第二控制指令,控制初始飞地的代理程序获取代理程序所预存的飞地原始ID,并根据飞地原始ID对待查询飞地ID进行位置验证,从而在待查询飞地ID位置验证通过时,输出第二验证信息。通过这一方法,本申请可以有效的对代理程序正在访问的初始飞地的身份合法性进行校验,从而对校验通过的初始飞地进行后续的自省操作。

[0044] 参照图6,在一些实施例中,步骤S180包括:

步骤S610,实时获取第三控制指令,当获取到第三控制指令时,执行以下步骤:

步骤S620,获取预设的加密密钥;

步骤S630,控制初始飞地的代理程序根据加密密钥对自省验证数据进行数据加密操作,得到第三验证信息。

[0045] 本申请所提供的飞地实时自省方法通过实时获取到的第三控制指令,调用代理程序预设的加密密钥,并根据代理程序根据加密密钥对自省验证数据进行加密操作,得到包含签名后的自省报告的第三验证信息,从而实现对初始飞地的实时自省。在一些具体的实施例中,加密密钥也可以存储在初始飞地的外部内存中,并通过代理程序对初始飞地的外部内存中的加密密钥进行调用,从而实现对自省验证数据的加密。

[0046] 第二方面,参照图7,本发明提供了一种飞地实时自省方法,应用于第二线程,包括:

步骤S710,根据预设的监控开始请求,检测共享内存的读写状态;其中共享内存存储有初始代码数据;

步骤S720,根据读写状态,实时获取飞地自省指令;

步骤S730,根据获取到的飞地自省指令,输出第一控制指令,并实时获取第一验证信息;

步骤S740,根据获取到的第一验证信息,输出第二控制指令,并实时获取第二验证信息;

步骤S750,根据获取到的第二验证信息,输出第三控制指令。

[0047] 本申请所提供的飞地实时自省方法,可以应用于第二线程,以使第二线程根据共享内存的读写状态和第一线程输出的验证信息输出对应的控制指令,以使第一线程可以控制指令对飞地进行实时自省。具体地,本方法可以根据预设的监控开始请求控制第二线程监控共享内存的读写状态。其中,共享内存存储有初始代码数据。并在检测到共享内存的读写状态为正在读写时,实时获取第一线程获取到的飞地自省指令,从而根据飞地自省指令输出第一控制指令,以控制第一线程根据第一控制指令输出第一验证信息,从而使第二线程通过实时监控第一验证信息获取第一验证信息;根据第一验证信息,本方法控制第二线程输出第二控制指令至第一线程,以使第一线程根据第二控制指令输出第二验证信息,从而使第二线程通过实时监控第二验证信息获取第二验证信息;通过第二验证信息,本方法可以控制第二线程将第三控制指令输出至第一线程,以使第一线程根据第三控制指令实现对自省验证数据的加密操作。通过这一方法,本申请可以有效的对共享内存内初始代码数据的调用状态进行监控,当监控到初始代码数据被第一线程调用时,可以根据第一线程的

执行状态输出不同的控制指令，以协助第一线程根据第二线程输出的第一控制指令或者第二控制指令或者第三控制指令执行相应的操作，从而实现对飞地的实时自省以及自省结果的加密。

[0048] 在一些具体的实施例中，本方法在步骤S710之前，还包括：获取监控开始请求，并根据监控开始请求调整共享内存权限。

[0049] 通过获取监控开始请求并调整共享内存权限，本方法可以对共享内存的读写权限进行限制，当调整共享内存权限后，本申请仅允许与飞地实时自省方法相关的线程对共享内存内的存储数据进行调用，从而保证共享内存内的存储数据的存储安全。

[0050] 在一些其他的实施例中，本申请可以通过第一控制指令控制第一线程对初始飞地的状态保存页面内存数据进行合法性检测；并在初始飞地的状态保存页面内存数据合法性检测通过后控制第一线程继续对锚代码数据和自省代码数据进行数据比对，并在锚代码数据和自省代码数据进行数据比对通过之后输出第一验证信息；

第三方面，参照图8，本发明提供了一种飞地实时自省装置，应用于第一线程，包括：

指令获取模块810，用于获取飞地自省指令；

代码获取模块820，用于获取原始飞地内预存的初始代码数据；

初始化模块830，用于根据飞地自省指令对原始飞地进行初始化操作，得到初始飞地；

第一验证模块840，用于根据获取到的第一控制指令和初始代码数据对初始飞地进行数据比对，得到第一验证信息；

第一数据模块850，用于根据第一验证信息和初始代码数据查询初始飞地的身份信息，得到待查询飞地ID；

第二验证模块860，用于根据获取到的第二控制指令对待查询飞地ID进行位置验证，得到第二验证信息；

第二数据模块870，用于根据第二验证信息对初始飞地进行自省操作，得到自省验证数据；

第三数据模块880，用于根据获取到的第三控制指令对自省验证数据进行数据加密操作，得到第三验证信息；其中，第三验证信息包括初始飞地的自省结果。

[0051] 根据本申请实施例应用于第一线程的飞地实时自省装置，通过指令获取模块810可以获取飞地自省指令，并将飞地自省指令输出至代码获取模块820以获取初始飞地内预存的初始代码数据；通过初始化模块830，本申请可以根据飞地自省指令对原始飞地进行初始化操作，从而生成初始飞地；通过第一验证模块840，本申请可以根据获取到的第一控制指令和初始代码数据对初始飞地进行数据比对，得到第一验证信息；通过第一数据模块850根据第一验证信息和初始代码数据对初始飞地的身份信息进行查询，得到待查询飞地ID；通过第二验证模块860，本装置可以获取到的第二控制指令对待查询飞地ID进行位置验证，得到第二验证信息；通过第二数据模块870，本装置可以根据第二验证信息对初始飞地进行自省操作，得到自省验证数据；通过第三数据模块880，本装置可以根据获取到的第三控制指令对自省验证数据进行数据加密操作，得到第三验证信息；其中，第三验证信息包括初始飞地的自省结果。通过本发明提供的应用于第一线程的飞地实时自省装置，本申请可以通

过对原始飞地进行初始化操作以更改飞地内数据的调用权限，校验初始代码数据的存储状态并通过飞地内预存的初始代码数据对初始飞地的身份信息进行查询，从而根据包含初始飞地身份信息的飞地ID对飞地进行检测，进而检测初始飞地的可信性，以对位置检测的初始飞地实现自省操作。本装置有效的实现了对初始飞地的自省，并通过对自行得到的自省验证数据加密得到第三验证信息，使得用户可以通过代理程序实时获取当前初始飞地的自省结果，避免了基于SGX本地/远程机制对飞地进行自省时，无法保证通信过程的安全性以及无法阻止非法攻击的风险，提供了一种更为安全的飞地实时自省装置。

[0052] 第四方面，参照图9，本发明提供了一种飞地实时自省装置，应用于第二线程，包括：

检测模块910，用于根据预设的监控开始请求，检测共享内存的读写状态；其中共享内存存储有初始代码数据；

指令生成模块920，用于根据读写状态，实时获取飞地自省指令；

第一输出模块930，用于根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；

第二输出模块940，用于根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；

第三输出模块950，用于根据获取到的第二验证信息，输出第三控制指令。

[0053] 根据本申请实施例应用于第一线程的飞地实时自省装置，本申请可以通过检测模块910实现根据预设的监控开始请求，检测共享内存的读写状态；其中共享内存存储有初始代码数据；通过指令生成模块920，本申请可以根据读写状态，实时获取飞地自省指令；通过第一输出模块930，本申请可以根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息；通过第二输出模块940，本申请可以根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息；通过第三输出模块950，本申请可以根据获取到的第二验证信息，输出第三控制指令。通过本申请提供的应用于第二线程的飞地实时自省装置，本发明可以使第二线程根据共享内存的读写状态和第一线程输出的验证信息输出对应的控制指令，以使第一线程可以控制指令对飞地进行实时自省。具体地，本装置可以根据预设的监控开始请求控制第二线程监控共享内存的读写状态。其中，共享内存存储有初始代码数据。并在检测到共享内存的读写状态为正在读写时，实时获取第一线程获取到的飞地自省指令，从而根据飞地自省指令输出第一控制指令，以控制第一线程根据第一控制指令输出第一验证信息，从而使第二线程通过实时监控第一验证信息获取第一验证信息；根据第一验证信息，本装置控制第二线程输出第二控制指令至第一线程，以使第一线程根据第二控制指令输出第二验证信息，从而使第二线程通过实时监控第二验证信息获取第二验证信息；通过第二验证信息，本装置可以控制第二线程将第三控制指令输出至第一线程，以使第一线程根据第三控制指令实现对自省验证数据的加密操作。通过这一装置，本申请可以有效的对共享内存内初始代码数据的调用状态进行监控，当监控到初始代码数据被第一线程调用时，可以根据第一线程的执行状态输出不同的控制指令，以协助第一线程根据第二线程输出的第一控制指令或者第二控制指令或者第三控制指令执行相应的操作，从而实现对飞地的实时自省以及自省结果的加密。

[0054] 第五方面，本发明提供了一种电子设备，包括：

至少一个存储器，以及

与至少一个存储器通信连接的处理器，其中；

至少一个存储器存储有计算机可执行指令，处理器用于执行计算机可执行指令，以使计算机执行计算机可执行指令时，实现如本发明第一方面的飞地实时自省方法，或者实现如本发明第二方面的飞地实时自省方法。

[0055] 该电子设备的具体实施方式与上述应用于第一线程的飞地实时自省方法的具体实施例，或者应用于第二线程的飞地实时自省方法的具体实施例基本相同，在此不再赘述。

[0056] 上面结合附图对本申请实施例作了详细说明，但是本申请不限于上述实施例，在所属技术领域普通技术人员所具备的知识范围内，还可以在不脱离本申请宗旨的前提下作出各种变化。此外，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

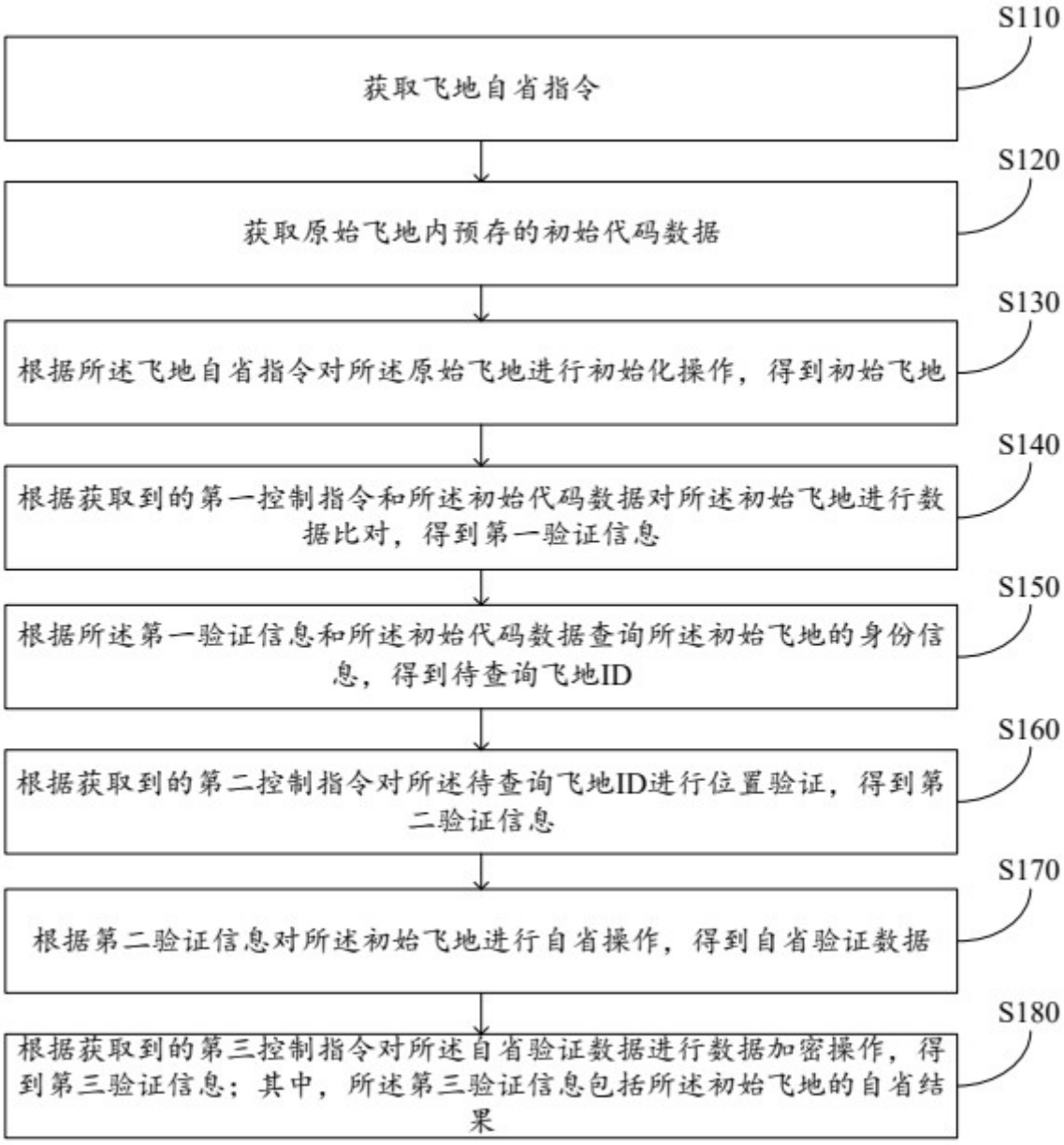

S110
获取飞地自省指令
S120
获取原始飞地内预存的初始代码数据
S130
根据所述飞地自省指令对所述原始飞地进行初始化操作，得到初始飞地
S140
根据获取到的第一控制指令和所述初始代码数据对所述初始飞地进行数据比对，得到第一验证信息
S150
根据所述第一验证信息和所述初始代码数据查询所述初始飞地的身份信息，得到待查询飞地ID
S160
根据获取到的第二控制指令对所述待查询飞地ID进行位置验证，得到第二验证信息
S170
根据第二验证信息对所述初始飞地进行自省操作，得到自省验证数据
S180
根据获取到的第三控制指令对所述自省验证数据进行数据加密操作，得到第三验证信息；其中，所述第三验证信息包括所述初始飞地的自省结果

图1

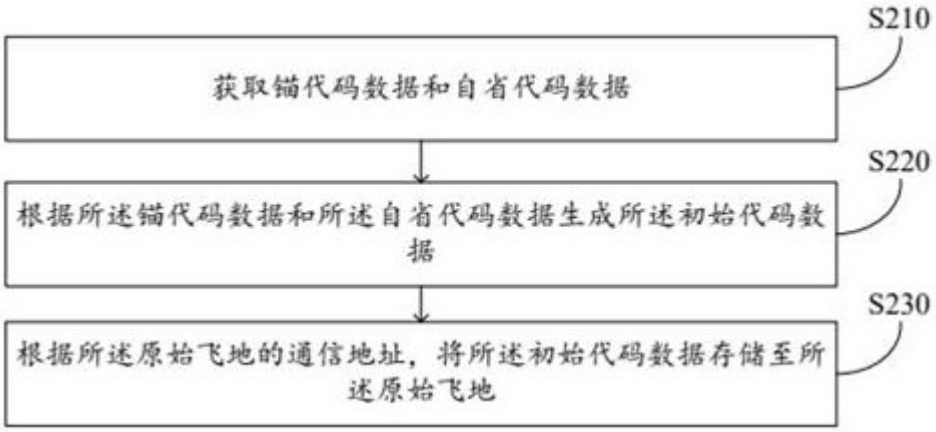

S210
获取锚代码数据和自省代码数据
S220
根据所述锚代码数据和所述自省代码数据生成所述初始代码数据
S230
根据所述原始飞地的通信地址，将所述初始代码数据存储至所述原始飞地

图2

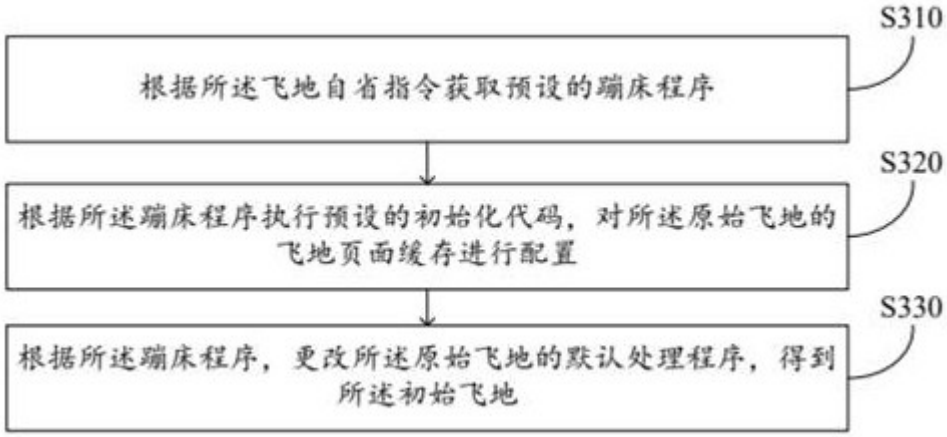

S310
根据所述飞地自省指令获取预设的蹦床程序
S320
根据所述蹦床程序执行预设的初始化代码，对所述原始飞地的飞地页面缓存进行配置
S330
根据所述蹦床程序，更改所述原始飞地的默认处理程序，得到所述初始飞地

图3

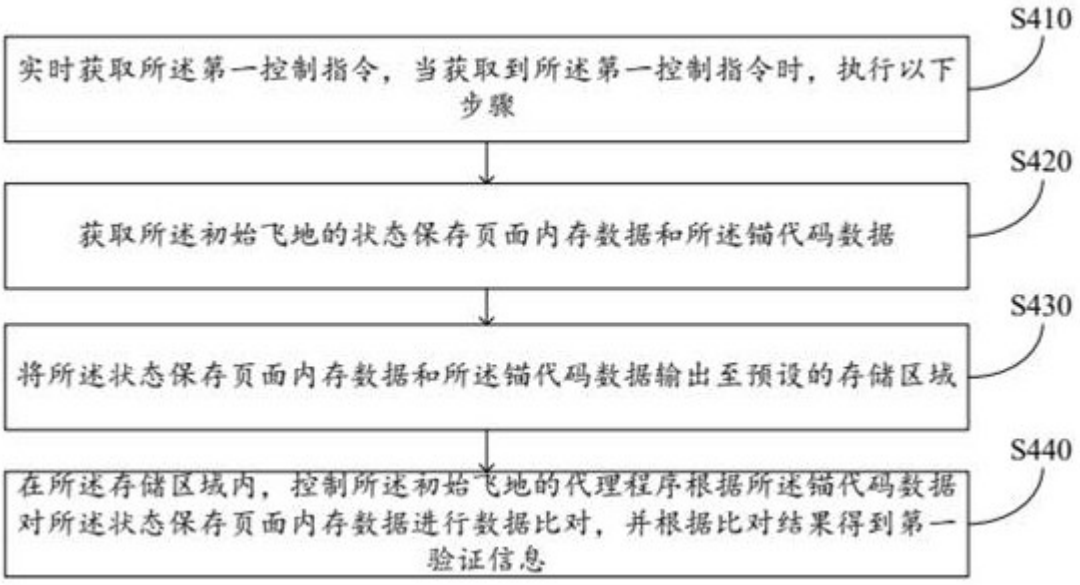

S410
实时获取所述第一控制指令，当获取到所述第一控制指令时，执行以下步骤
S420
获取所述初始飞地的状态保存页面内存数据和所述锚代码数据
S430
将所述状态保存页面内存数据和所述锚代码数据输出至预设的存储区域
S440
在所述存储区域内，控制所述初始飞地的代理程序根据所述锚代码数据对所述状态保存页面内存数据进行数据比对，并根据比对结果得到第一验证信息

图4

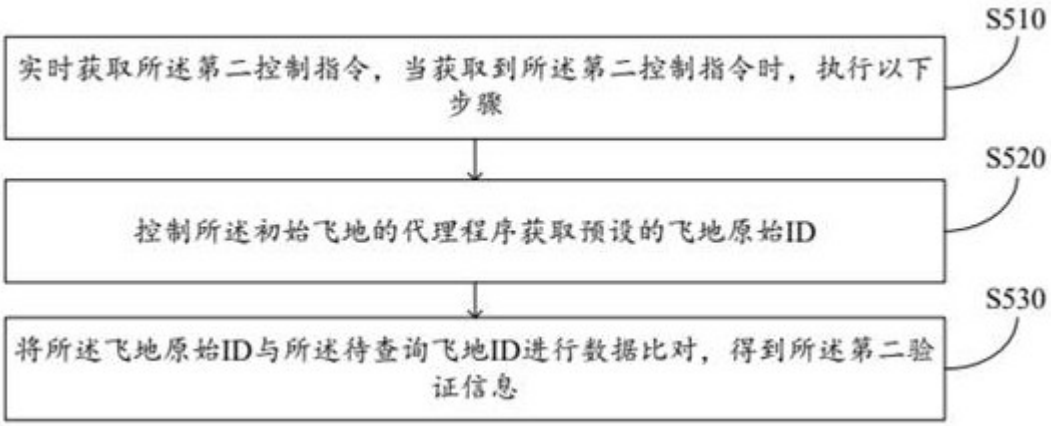

S510
实时获取所述第二控制指令，当获取到所述第二控制指令时，执行以下步骤
S520
控制所述初始飞地的代理程序获取预设的飞地原始ID
S530
将所述飞地原始ID与所述待查询飞地ID进行数据比对，得到所述第二验证信息

图5

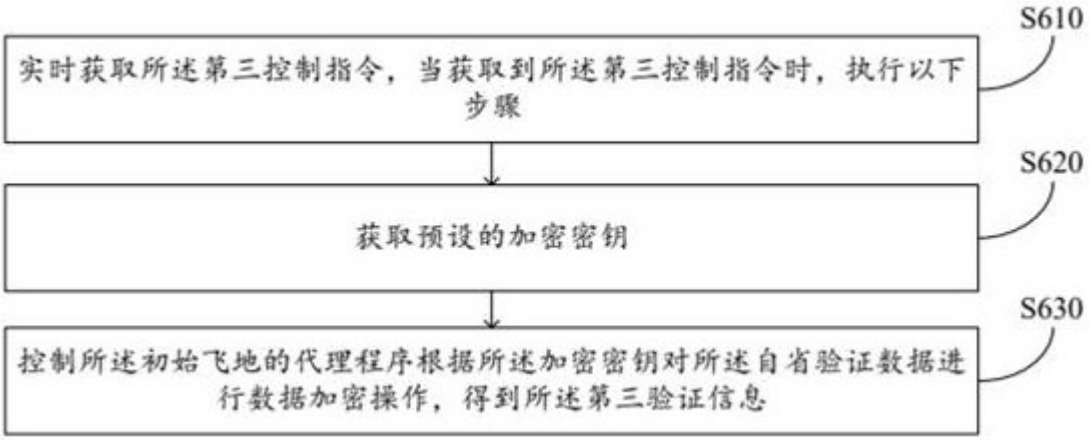

S610
实时获取所述第三控制指令，当获取到所述第三控制指令时，执行以下步骤
S620
获取预设的加密密钥
S630
控制所述初始飞地的代理程序根据所述加密密钥对所述自省验证数据进行数据加密操作，得到所述第三验证信息

图6

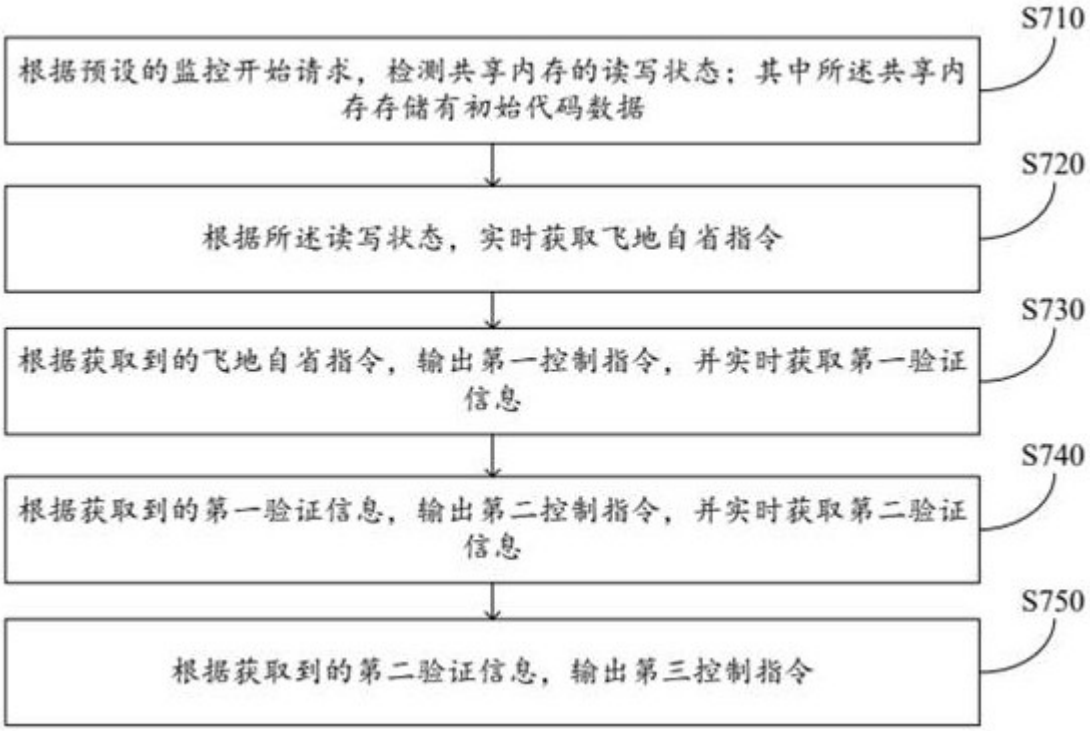

S710
根据预设的监控开始请求，检测共享内存的读写状态；其中所述共享内存存储有初始代码数据
S720
根据所述读写状态，实时获取飞地自省指令
S730
根据获取到的飞地自省指令，输出第一控制指令，并实时获取第一验证信息
S740
根据获取到的第一验证信息，输出第二控制指令，并实时获取第二验证信息
S750
根据获取到的第二验证信息，输出第三控制指令

图7

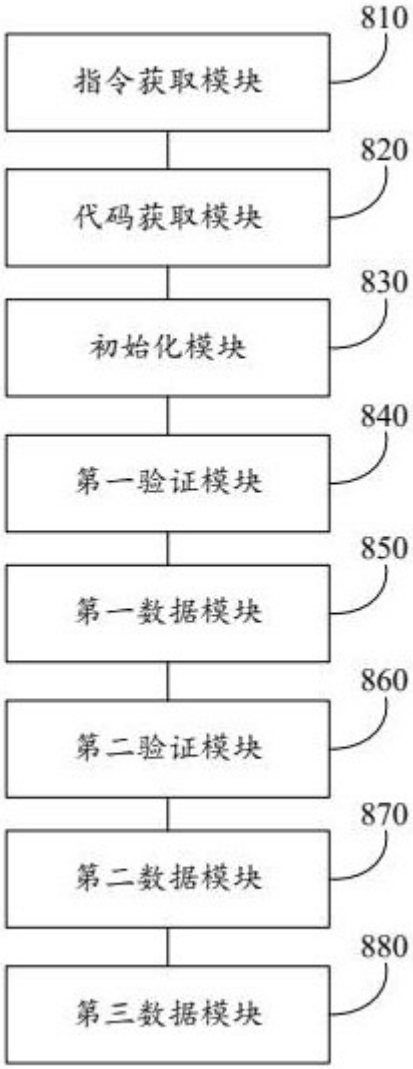

810
指令获取模块
820
代码获取模块
830
初始化模块
840
第一验证模块
850
第一数据模块
860
第二验证模块
870
第二数据模块
880
第三数据模块

图8

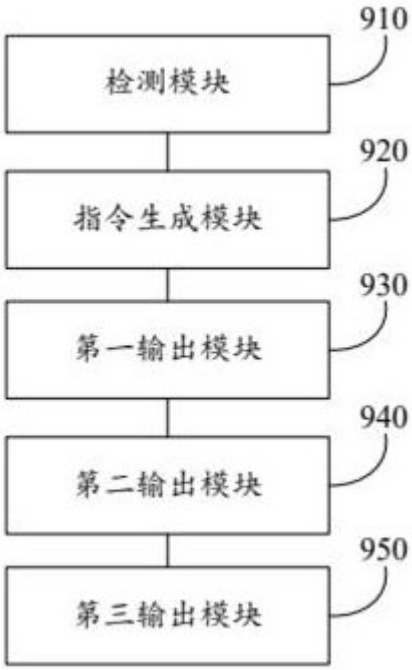


图9