(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 111143887 A
(43)申请公布日 2020.05.12

(21)申请号 201911342360.9

(22)申请日 2019.12.26

(71)申请人 海光信息技术有限公司
地址 300450 天津市滨海新区华苑产业区海泰西路18号北2-204工业孵化-3-8

(72)发明人 陈善

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 蒋姗

(51)Int.Cl.
G06F 21/64(2013.01)
G06F 21/62(2013.01)
G06F 21/57(2013.01)

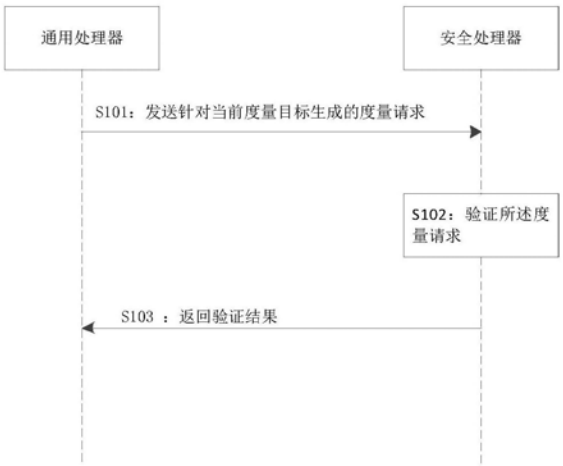
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种安全控制方法、处理器、集成器件及计算机设备

(57)摘要

本申请涉及一种安全控制方法、处理器、集成器件及计算机设备，属于计算机技术领域。该方法包括：接收针对当前度量目标生成的度量请求，度量请求基于签名链生成，签名链包括与多个度量目标一一对应且按照多个度量目标的设定顺序排列的多个签名单元，度量请求包括与当前度量目标对应的当前签名单元；根据当前签名单元和本地存储的本地签名单元，验证度量请求；在验证通过时，用当前签名单元更新本地签名单元；输出验证结果。本申请通过签名链将各度量目标有机串联起来，使得对各度量目标严格按照签名链上的顺序依次进行完整性与依赖性双重度量，度量目标不可被绕过也不可被替换，保证了系统的整体完整性和一致性，进一步增强了系统启动安全。



CN 111143887 A

1.一种安全控制方法,其特征在于,包括:

接收针对当前度量目标生成的度量请求,所述度量请求基于签名链生成,所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元,所述当前度量目标为所述多个度量目标中的一个度量目标,所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元;

根据所述当前签名单元和本地存储的本地签名单元,验证所述度量请求,其中,所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元;

在验证通过时,用所述当前签名单元更新所述本地签名单元;

输出验证结果。

2.根据权利要求1所述的方法,其特征在于,所述签名链中的每个签名单元包括:签名链识别号;验证所述度量请求,包括:

验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致;

在为是时,表征验证通过。

3.根据权利要求1所述的方法,其特征在于,所述签名链中的每个签名单元包括:签名值和该签名单元对应的度量目标的Hash值,其中,所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进行加密签名生成的值,i为大于等于1的正整数;验证所述度量请求,包括:

根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值;

解密所述当前签名单元中的签名值,并验证所述待验证扩展值与解密后的签名值是否一致;或者,验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致;

在所述待验证扩展值与解密后的签名值一致时,或者,在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时,表征验证通过。

4.根据权利要求3所述的方法,其特征在于,所述签名链中的每个签名单元还包括:签名链识别号;在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前,所述方法还包括:

确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。

5.根据权利要求1-4中任一项所述的方法,其特征在于,所述度量请求还包括所述当前度量目标;在验证所述度量请求之前,所述方法还包括:

计算所述当前度量目标的Hash值;

确定所述当前签名单元中的Hash值与计算出的Hash值一致。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

接收查询请求,所述查询请求包括请求类型,所述请求类型用于指示查询本地存储的本地签名单元;

响应所述查询请求,返回所述本地存储的本地签名单元。

7.根据权利要求1所述的方法,其特征在于,所述签名链中的多个签名单元为按照系统

启动时的度量目标的启动顺序排列的多个度量目标一一对应的多个签名单元。

8.一种安全控制方法,其特征在于,

计算当前度量目标的Hash值;

从签名链中查找与所述Hash值匹配的当前签名单元,其中,所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元,所述当前度量目标为所述多个度量目标中的一个度量目标;

生成并发送度量请求,所述度量请求包括:所述当前度量目标和所述当前签名单元。

9.一种处理器,其特征在于,包括:

处理器核,用于针对当前度量目标生成度量请求,并发送所述度量请求,所述度量请求基于签名链生成,所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元,所述当前度量目标为所述多个度量目标中的一个度量目标,所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元;

安全处理器,用于接收所述度量请求并根据所述当前签名单元和本地存储的本地签名单元,验证所述度量请求,以及在验证通过时,用所述当前签名单元更新所述本地签名单元;以及还用于发送验证结果,其中,所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元。

10.根据权利要求9所述的处理器,其特征在于,所述签名链中的每个签名单元包括:签名链识别号;所述安全处理器,用于验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致;在为是时,表征验证通过。

11.根据权利要求9所述的处理器,其特征在于,所述签名链中的每个签名单元包括:签名值和该签名单元对应的度量目标的Hash值,其中,所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进行加密签名生成的值,i为大于等于1的正整数;所述安全处理器,用于:

根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值;

解密所述当前签名单元中的签名值,并验证所述待验证扩展值与解密后的签名值是否一致;或者,验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致;

在所述待验证扩展值与解密后的签名值一致时,或者,在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时,表征验证通过。

12.根据权利要求11所述的处理器,其特征在于,所述签名链中的每个签名单元还包括:签名链识别号;所述安全处理器,还用于在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前,确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。

13.根据权利要求9-12任一项所述的处理器,其特征在于,所述度量请求还包括所述当前度量目标,所述安全处理器,还用于在验证所述度量请求之前,计算所述当前度量目标的Hash值,并确定所述当前签名单元中的Hash值与计算出的Hash值一致。

14.根据权利要求9所述的处理器,其特征在于,所述处理器核,还用于向所述安全处理器发送查询请求,所述查询请求包括请求类型,所述请求类型用于指示查询本地存储的本

地签名单元；

所述安全处理器，还用于响应所述查询请求，返回所述本地存储的本地签名单元。

15.一种集成器件，其特征在于，包括：

通用处理器，用于针对当前度量目标生成度量请求，并发送所述度量请求，所述度量请求基于签名链生成，所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元，所述当前度量目标为所述多个度量目标中的一个度量目标，所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元；

安全处理器，用于接收所述度量请求并根据所述当前签名单元和本地存储的本地签名单元，验证所述度量请求，以及在验证通过时，用所述当前签名单元更新所述本地签名单元；以及还用于发送验证结果，其中，所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元。

16.根据权利要求15所述的集成器件，其特征在于，所述签名链中的每个签名单元包括：签名链识别号；所述安全处理器，用于验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致；在为是时，表征验证通过。

17.根据权利要求15所述的集成器件，其特征在于，所述签名链中的每个签名单元包括：签名值和该签名单元对应的度量目标的Hash值，其中，所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进行加密签名生成的值，i为大于等于1的正整数；所述安全处理器，用于：

根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；

解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致；

在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。

18.根据权利要求17所述的集成器件，其特征在于，所述签名链中的每个签名单元还包括：签名链识别号；所述安全处理器，还用于在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前，确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。

19.根据权利要求15-18任一项所述的集成器件，其特征在于，所述度量请求还包括所述当前度量目标，所述安全处理器，还用于在验证所述度量请求之前，计算所述当前度量目标的Hash值，并确定所述当前签名单元中的Hash值与计算出的Hash值一致。

20.根据权利要求15所述的集成器件，其特征在于，所述通用处理器，还用于向所述安全处理器发送查询请求，所述查询请求包括请求类型，所述请求类型用于指示查询本地存储的本地签名单元；

所述安全处理器，还用于响应所述查询请求，返回所述本地存储的本地签名单元。

21.一种计算机设备，其特征在于，包括：如权利要求9-14任一项所述的处理器，或者，如权利要求15-20任一项所述的集成器件。

一种安全控制方法、处理器、集成器件及计算机设备

技术领域

[0001] 本申请属于计算机技术领域，具体涉及一种安全控制方法、处理器、集成器件及计算机设备。

背景技术

[0002] 计算机系统的主要工作是执行程序，正常情况下，程序代码及其配置参数应保持不变，程序每次执行的行为应完全一样。然而由于设计或者实现上的缺陷，程序有可能发生改变，一旦程序发生改变，容易导致计算机系统的行为发生失控。为了避免上述情况的发生，计算机在启动时采用静态度量的方法对程序文件进行完整性检验，保证程序所执行的文件未被篡改。现有技术中通常以隔离的方式验证各个度量目标的签名是否有效，度量目标是否验证成功取决于目标本身。上述方法在系统整体完整性和一致性的度量及保护上存在不足：某些度量目标在签名合法的情况下容易被替换；系统启动时即便绕过了某些度量目标，如某些设备的配置文件，系统无法知晓并采取措施。

发明内容

[0003] 鉴于此，本申请的目的在于提供一种安全控制方法、处理器、集成器件及计算机设备，以增强系统的启动安全。

[0004] 本申请的实施例是这样实现的：

[0005] 第一方面，本申请实施例提供了一种安全控制方法，包括：接收针对当前度量目标生成的度量请求，所述度量请求基于签名链生成，所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元，所述当前度量目标为所述多个度量目标中的一个度量目标，所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元；根据所述当前签名单元和本地存储的本地签名单元，验证所述度量请求，其中，所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元；在验证通过时，用所述当前签名单元更新所述本地签名单元；输出验证结果。本申请通过签名链将各度量目标有机串联起来，使得对各度量目标严格按照签名链上的顺序依次进行完整性与依赖性双重度量，度量目标不可被绕过也不可被替换，保证了系统的整体完整性和一致性，进一步增强了系统启动安全。

[0006] 结合第一方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名链识别号；验证所述度量请求，包括：验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致；在为是时，表征验证通过。本申请实施例中，通过验证当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致，即以快速的得到验证结果。

[0007] 结合第一方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名值和该签名单元对应的度量目标的Hash值，其中，所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进

行加密签名生成的值，i为大于等于1的正整数；验证所述度量请求，包括：根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致；在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。本申请实施例中，通过采用第i个签名单元的签名值为对根据第i个和第i-1个签名单元的度量目标的Hash值计算得到的扩展值进行加密签名生成的值的方式，充分考虑了各度量目标之间的关联性，使得任一签名的变动都会导致签名链的破坏，从而保证签名链的整体完整性和一致性，进而保证启动过程的绝对受控和安全。

[0008] 结合第一方面实施例的一种可能的实施方式，所述签名链中的每个签名单元还包括：签名链识别号；在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前，所述方法还包括：确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。本申请实施例中，在根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值之前，先验证当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致，只有在确定当前签名单元中的签名链识别号与本地签名单元中的签名链识别号一致后，才进行后续的验证，在保证签名链的整体完整性和一致性的前提下，可以避免不必要的验证流程。

[0009] 结合第一方面实施例的一种可能的实施方式，所述度量请求还包括所述当前度量目标；在验证所述度量请求之前，所述方法还包括：计算所述当前度量目标的Hash值；确定所述当前签名单元中的Hash值与计算出的Hash值一致。本申请实施例中，在对度量请求进行验证之前，需要先确保计算得到的当前度量目标的Hash值与当前签名单元中的Hash值一致，当计算的Hash值与当前签名单元中的Hash值不一致时，便可直接得出验证失败的结论，从而不需要再进行后续的验证流程。

[0010] 结合第一方面实施例的一种可能的实施方式，所述方法还包括：接收查询请求，所述查询请求包括请求类型，所述请求类型用于指示查询本地存储的本地签名单元；响应所述查询请求，返回所述本地存储的本地签名单元。本申请实施例中，通过查询本地存储的本地签名单元，结合签名链判断系统启动到了哪个阶段，是否完成了所有预设目标的度量，为判断系统整体健康状况提供依据。

[0011] 结合第一方面实施例的一种可能的实施方式，所述签名链中的多个签名单元为按照系统启动时的度量目标的启动顺序排列的多个度量目标一一对应的多个签名单元。本申请实施例中，该签名链中的多个签名单元为按照系统启动时的度量目标的启动顺序排列的多个度量目标一一对应的多个签名单元，使得在系统启动时，对各度量目标严格按照签名链上的顺序依次进行完整性与依赖性双重度量，度量目标不可被绕过也不可被替换，保证了系统的整体完整性和一致性，进一步增强了系统启动安全。

[0012] 第二方面，本申请实施例还提供了一种安全控制方法，计算当前度量目标的Hash值；从签名链中查找与所述Hash值匹配的当前签名单元，其中，所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元，所述当前度量目标为所述多个度量目标中的一个度量目标；生成并发送度量请求，所述度量请求包括：所述

当前度量目标和所述当前签名单元。本申请实施例中，通过签名链将各度量目标有机串联起来，使得在对当前度量目标进行验证时，通过从签名链中查找与计算得到的当前度量目标的Hash值匹配的当前签名单元，来生成度量请求，使得对当前度量目标严格按照签名链上的顺序进行完整性与依赖性双重度量，度量目标不可被绕过也不可被替换，保证了系统的整体完整性和一致性，进一步增强了系统启动安全。

[0013] 第三方面，本申请实施例还提供了一种处理器，包括：处理器核和安全处理器；处理器核，用于针对当前度量目标生成度量请求，并发送所述度量请求，所述度量请求基于签名链生成，所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元，所述当前度量目标为所述多个度量目标中的一个度量目标，所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元；安全处理器，用于接收所述度量请求并根据所述当前签名单元和本地存储的本地签名单元，验证所述度量请求，以及在验证通过时，用所述当前签名单元更新所述本地签名单元；以及还用于发送验证结果，其中，所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元。

[0014] 结合第三方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名链识别号；所述安全处理器，用于验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致；在为是时，表征验证通过。

[0015] 结合第三方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名值和该签名单元对应的度量目标的Hash值，其中，所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进行加密签名生成的值，i为大于等于1的正整数；所述安全处理器，用于：根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致；在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。

[0016] 结合第三方面实施例的一种可能的实施方式，所述签名链中的每个签名单元还包括：签名链识别号；所述安全处理器，还用于在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前，确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。

[0017] 结合第三方面实施例的一种可能的实施方式，所述度量请求还包括所述当前度量目标，所述安全处理器，还用于在验证所述度量请求之前，计算所述当前度量目标的Hash值，并确定所述当前签名单元中的Hash值与计算出的Hash值一致。

[0018] 结合第三方面实施例的一种可能的实施方式，所述处理器核，还用于向所述安全处理器发送查询请求，所述查询请求包括请求类型，所述请求类型用于指示查询本地存储的本地签名单元；所述安全处理器，还用于响应所述查询请求，返回所述本地存储的本地签名单元。

[0019] 第四方面，本申请实施例还提供了一种集成器件，包括：通用处理器和安全处理器；通用处理器，用于针对当前度量目标生成度量请求，并发送所述度量请求，所述度量请求基于签名链生成，所述签名链包括与多个度量目标一一对应且按照所述多个度量目标的

设定顺序排列的多个签名单元，所述当前度量目标为所述多个度量目标中的一个度量目标，所述度量请求包括所述签名链中与所述当前度量目标对应的当前签名单元；安全处理器，用于接收所述度量请求并根据所述当前签名单元和本地存储的本地签名单元，验证所述度量请求，以及在验证通过时，用所述当前签名单元更新所述本地签名单元；以及还用于发送验证结果，其中，所述本地签名单元为所述签名链中所述当前签名单元的前一个签名单元。

[0020] 结合第四方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名链识别号；所述安全处理器，用于验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致；在为是时，表征验证通过。

[0021] 结合第四方面实施例的一种可能的实施方式，所述签名链中的每个签名单元包括：签名值和该签名单元对应的度量目标的Hash值，其中，所述签名链中第i个签名单元的签名值是对根据第i个和第i-1个签名单元对应的度量目标的Hash值计算得到的扩展值进行加密签名生成的值，i为大于等于1的正整数；所述安全处理器，用于：根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值是否一致；在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行所述加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。

[0022] 结合第四方面实施例的一种可能的实施方式，所述签名链中的每个签名单元还包括：签名链识别号；所述安全处理器，还用于在根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值之前，确定所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号一致。

[0023] 结合第四方面实施例的一种可能的实施方式，所述度量请求还包括所述当前度量目标，所述安全处理器，还用于在验证所述度量请求之前，计算所述当前度量目标的Hash值，并确定所述当前签名单元中的Hash值与计算出的Hash值一致。

[0024] 结合第四方面实施例的一种可能的实施方式，所述通用处理器，还用于向所述安全处理器发送查询请求，所述查询请求包括请求类型，所述请求类型用于指示查询本地存储的本地签名单元；所述安全处理器，还用于响应所述查询请求，返回所述本地存储的本地签名单元。

[0025] 第五方面，本申请实施例还提供了一种计算机设备，包括：如上述第三方面实施例和/或结合第三方面实施例的任一种可能的实施方式提供的处理器，或者，如上述第四方面实施例和/或结合第四方面实施例的任一种可能的实施方式提供的集成器件。

[0026] 本申请的其他特征和优点将在随后的说明书阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请实施例而了解。本申请的目的和其他优点可通过在所写的说明书以及附图中所特别指出的结构来实现和获得。

附图说明

[0027] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例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申请的一些实施

例，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。通过附图所示，本申请的上述及其它目的、特征和优势将更加清晰。在全部附图中相同的附图标记指示相同的部分。并未刻意按实际尺寸等比例缩放绘制附图，重点在于示出本申请的主旨。

[0028] 图1示出了本申请实施例提供的一种计算机设备的结构框图。

[0029] 图2示出了本申请实施例提供的一种签名链的结构示意图。

[0030] 图3示出了本申请实施例提供的一种安全控制方法的交互示意图。

[0031] 图4示出了本申请实施例提供的又一种安全控制方法的交互示意图。

具体实施方式

[0032] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。

[0033] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。同时，在本申请的描述中诸如“第一”、“第二”等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0034] 再者，本申请中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。

[0035] 计算机在启动时，为了保证系统启动的安全性，需要对程序文件进行安全度量以保证程序所执行的文件未被篡改。发明人在研究本申请的过程中发现，现有技术中通常以隔离的方式验证单个度量目标的签名是否有效，而各度量目标之间相互独立，没有关联性，度量目标是否验证成功只取决于目标本身，与其他度量目标无关。现有的这种验证方式在系统整体完整性和一致性的度量及保护上存在不足：单个度量目标在签名合法的情况下容易被替换；系统启动时即便绕过了某些度量目标，如某些设备的配置文件，系统无法知晓并采取措施。其中，需要说明的是，针对以上方案所存在的缺陷，均是发明人在经过实践并仔细研究后得出的结果，因此，上述问题的发现过程以及下文中本申请实施例针对上述问题所提出的解决方案，都应该是发明人在本申请过程中对本申请做出的贡献。

[0036] 鉴于此，本申请提供一种计算机安全控制方法，基于系统中配置的签名链对各度量目标按照固定的顺序进行完整性和依赖性双重度量，度量目标不可被绕过也不可被替换，从而保证了系统的整体完整性和一致性，进一步增强了系统的启动安全。其中，各度量目标可以为镜像文件、配置文件或者设备固件等。

[0037] 图1示出了本申请实施例提供的一种计算机设备100的结构框图。该计算机设备100包括：通用处理器110、安全处理器120和内存130。其中，安全处理器120和通用处理器110可以是独立的两个集成芯片，两者均集成在主板上，构成一个集成器件(如SOC芯片)，也即该集成器件包括：通用处理器110和安全处理器120。其中，SOC(System on Chip)指的是

片上系统，也称为系统级芯片。一种实施方式下，该安全处理器120也可以是集成在通用处理器110中，如Dhyana系列处理器。

[0038] 安全处理器120具有专属的硬件资源，如运行内存、非易失存储器等，上述硬件资源与通用处理器110隔离，通用处理器110不可访问上述硬件资源。安全处理器120与通用处理器110之间通过固定的通信接口进行通信，同时安全处理器120能够通过高速总线接收通用处理器110传过来的数据或者直接访问通用处理器110指定的内存130中的内存地址。安全处理器120能够及时接收通用处理器110通过固定的通信接口发送过来的命令，并在执行该命令后将执行结果返回给通用处理器110。

[0039] 其中，上述的通用处理器110可以是中央处理器(Central Processing Unit，CPU)、图形处理器(Graphics Processing Unit，GPU)、加速处理器(Accelerated Processing Unit)等，也还可以是其他类型的处理器，如网络处理器(Network Processor，NP)、应用处理器，当然在某些产品中，应用处理器就是CPU。

[0040] 其中，内存130用于暂时存放处理器(通用处理器110、安全处理器120)需要的运算数据，以及与硬盘等外部存储器交换的数据，该内存可以是双倍速率同步动态随机存储器(Double Data Rate，DDR)，也还可以是其他的存储器，如随机存取存储器(Random Access Memory，RAM)，动态随机存储器(Dynamic Random Access Memory，DRAM)等。

[0041] 本申请通过签名链将各度量目标有机串联起来，目的在于建立启动过程各度量目标对应的签名之间的先后顺序及不可更改性，启动时利用安全处理器120对各度量目标严格按照签名链上的顺序依次进行验证，任一签名的变动都会导致签名链的破坏，从而保证签名链的整体完整性和一致性，进而保证启动过程的绝对受控和安全。

[0042] 图2示出了本申请实施例提供的一种签名链的结构示意图。签名链的实现形式较为灵活，本实施例中，签名链可以包括多个签名单元，每个签名单元具有一个编号，这里的编号可以为0，1，2...n，多个签名单元分别与多个度量目标一一对应，并且多个签名单元按照设定顺序排列，也即签名链中的多个签名单元为按照系统启动时的度量目标的启动顺序排列的多个度量目标一一对应的多个签名单元。各签名单元具有相同的数据结构，可以包括签名链识别号(Signature Chain Identifier，SCID)、签名值以及度量目标的Hash值等信息。其中，SCID可以用来标记该签名单元属于该签名链，SCID可以使用识别码生成工具UUID(Universally Unique Identifier)生成。度量目标的Hash值可以使用哈希算法(SM3算法)生成。第i个签名单元的签名值可以是对根据第i个签名单元的度量目标的Hash值和第i-1个签名单元的度量目标的Hash值计算得到的扩展值进行加密签名生成的值，i为大于等于1的正整数。这里，加密签名可以采用非对称密码算法，例如可以为SM2算法。需要注意的是，对于签名链中的第一个签名单元，该签名单元的签名值可以为采用非对称密码算法对该签名单元的度量目标的Hash值进行加密签名得到的。本申请的签名链可以位于通用处理器110的非易失存储器中，如硬盘或者Flash(闪存)，以方便系统更新时签名链的整体更新，签名链也可以存储在其他存储模块中，通用处理器110可以访问该模块得到签名链。特别地，每个签名单元还可以包括其他信息，如Hash算法、签名算法和公钥信息等。

[0043] 本申请实施例中的生成签名值所采用的私钥可由可信软件提供方安全保管，用来验证签名值的公钥可以位于安全处理器120内部，可以通过安全处理器120提供的安全命令接口进行修改。另外，系统初始安装时使用可信软件提供方提供的安装包，包括所有镜像文

件及度量目标的签名单元组成的签名链;系统更新时,比如升级操作系统(OS),可信软件提供方必须根据新的度量目标生成整个签名链,所有签名单元使用新的签名链识别号SCID,然后将更新后的镜像及签名链安装到要更新的系统上。

[0044] 系统启动时,通用处理器110针对当前度量目标生成度量请求,并将度量请求发送给安全处理器120。这里,度量请求可以基于签名链生成,具体为通用处理器110计算当前度量目标的Hash值,在签名链中查找Hash值与计算出的Hash值一致的签名单元,即为当前签名单元,基于查找到的当前签名单元生成度量请求。其中,度量请求包括该当前签名单元。其中,需要说明的是,当安全处理器120集成在通用处理器110中时,此时,生成度量请求这一动作由通用处理器110中的处理器核来完成,也即处理器核针对当前度量目标生成度量请求,并发送度量请求。

[0045] 安全处理器120接收到当前度量目标对应的度量请求,并验证该度量请求。在验证时,安全处理器120根据当前签名单元和本地存储的本地签名单元对该度量请求进行验证,并在验证通过后,用当前签名单元更新本地签名单元;以及还用于向通用处理器110发送验证结果。其中,安全处理器120可以具有签名单元缓存区(Signature Unit Buffer,SUB),当度量目标验证通过时,将该度量目标对应的签名单元保存至该签名单元缓存区,签名单元缓存区保存的签名单元即为本地签名单元。签名单元缓存区SUB在系统重启之前始终保存最近一次成功度量的签名单元。其中,若验证该度量请求为安全处理器120的第一次验证,也即此时签名单元缓存区中没有本地签名单元时,此时,安全处理器120直接基于当前签名单元验证当前度量目标的Hash值及签名值,例如,计算当前度量目标的Hash值,并验证当前签名单元中的Hash值与计算出的Hash值是否一致。此时,该度量请求包括当前度量目标和当前度量目标对应的当前签名单元。

[0046] 作为一种实施方式,当签名链中的每个签名单元均包括:签名链识别号时,安全处理器120,通过验证当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致;在为是(一致)时,表征验证通过。

[0047] 作为又一种实施方式,当签名链中的每个签名单元均包括:签名值和该签名单元对应的度量目标的Hash值时,在验证度量请求时,安全处理器120,用于根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值;解密当前签名单元中的签名值,并验证待验证扩展值与解密后的签名值是否一致;在待验证扩展值与解密后的签名值一致时,表征验证通过。或者,安全处理器120,用于根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值;验证对待验证扩展值进行加密签名生成的值与当前签名单元中的签名值是否一致;在对待验证扩展值进行加密签名生成的值与当前签名单元中的签名值一致时,表征验证通过。

[0048] 作为又一种实施方式,当签名链中的每个签名单元均包括:签名链识别号、签名值和该签名单元对应的度量目标的Hash值时,此时,安全处理器120,在根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值之前,先验证当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致,只有在确定当前签名单元中的签名链识别号与本地签名单元中的签名链识别号一致时(否则,直接得出验证失败的结论),才进行后续的验证,如进行根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值等动作。

[0049] 作为又一种实施方式，该度量请求还包括当前度量目标，也即，该度量请求包括当前度量目标和当前度量目标对应的当前签名单元，此时，该安全处理器120在验证度量请求之前，先计算当前度量目标的Hash值，并验证当前签名单元中的Hash值与计算出的Hash值是否一致，只有在确定当前签名单元中的Hash值与计算出的Hash值一致时，才验证度量请求，否则，直接得出验证失败的结论。

[0050] 从上面的实施方式可以看出，不同的验证方式，对应的签名链中的各个签名单元的所包含的信息可以不同，以及度量请求包含的内容也可以不同。因此，不能将上述示例的签名链理解成是对本申请的限制。

[0051] 为了便于判断系统启动到了哪个阶段，该通用处理器110还可以向安全处理器120发送查询请求，该查询请求包括用于指示查询本地存储的本地签名单元的请求类型。安全处理器120，在接收到该查询请求后，识别出该查询请求为查询本地存储的本地签名单元的请求时，响应该查询请求，向通用处理器110返回本地存储的本地签名单元，以使通用处理器110基于该本地签名单元结合签名链判断系统启动到了哪个阶段，是否完成了所有预设目标的度量，为上层应用判断系统整体健康状况提供依据。其中，需要说明的是，当安全处理器120集成在通用处理器110中时，此时，发送查询请求这一动作由通用处理器110中的处理器核来完成，也即处理器核向安全处理器120发送查询请求。

[0052] 请参阅图3，为本申请实施例提供的一种安全控制方法，下面将结合图3对其所包含的步骤进行说明。

[0053] 步骤S101：发送针对当前度量目标生成的度量请求。

[0054] 计算当前度量目标的Hash值，从签名链中查找与该Hash值匹配的当前签名单元，生成并发送度量请求，一种实施方式下，所述度量请求包括：当前度量目标对应的当前签名单元。

[0055] 其中，签名链包括与多个度量目标一一对应且按照所述多个度量目标的设定顺序排列的多个签名单元，可选地，签名链中的多个签名单元为按照系统启动时的度量目标的启动顺序排列的多个度量目标一一对应的多个签名单元。所述当前度量目标为所述多个度量目标中的一个度量目标。

[0056] 步骤S102：验证所述度量请求。

[0057] 安全处理器接收针对当前度量目标生成的度量请求，并根据当前签名单元和本地存储的本地签名单元验证该度量请求，若当前验证为第一次验证，本地存储的本地签名单元为空，此时相当于仅根据当前签名单元验证该度量请求，其过程可以是：对当前签名单元的签名值利用公钥进行解密，验证解密后的值和当前签名单元的度量目标的Hash值是否一致；若一致，则验证成功，否则，验证失败；或者，验证对当前签名单元的度量目标的Hash值进行加密签名生成的值和当前签名单元的签名值是否一致；若一致，则验证成功，否则，验证失败。在验证成功时，还基于当前签名单元更新本地签名单元。需要说明的是，判断当前验证是否是第一次验证的依据可以是，根据系统是否重启来判断，当系统刚重启时，便接收到度量请求，则当前验证即为第一次验证，否则，当前验证不是第一次验证。

[0058] 若当前验证不为第一次验证，此时本地存储的本地签名单元不为空，则根据当前签名单元和本地存储的本地签名单元，验证度量请求，得到验证通过(成功)或验证失败的验证结果。

[0059] 一种实施方式下，签名链中的每个签名单元包括：签名链识别号时；此时，验证所述度量请求的过程可以是：验证所述当前签名单元中的签名链识别号与所述本地签名单元中的签名链识别号是否一致；在为是时，表征验证通过。

[0060] 又一种实施方式下，所述签名链中的每个签名单元包括：签名值和该签名单元对应的度量目标的Hash值；验证所述度量请求的过程可以是：根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行加密签名生成的值与所述当前签名单元中的签名值是否一致；在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。

[0061] 又一种实施方式下，所述签名链中的每个签名单元包括：签名链识别号、签名值和该签名单元对应的度量目标的Hash值；验证所述度量请求的过程可以是：判断当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致，在为是时，根据所述当前签名单元中的Hash值和所述本地签名单元中的Hash值计算待验证扩展值；解密所述当前签名单元中的签名值，并验证所述待验证扩展值与解密后的签名值是否一致；或者，验证对所述待验证扩展值进行加密签名生成的值与所述当前签名单元中的签名值是否一致；在所述待验证扩展值与解密后的签名值一致时，或者，在对所述待验证扩展值进行加密签名生成的值与所述当前签名单元中的签名值一致时，表征验证通过。也即在该实施方式中，在根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值之前，先验证当前签名单元中的签名链识别号与本地签名单元中的签名链识别号是否一致，只有在确定当前签名单元中的签名链识别号与本地签名单元中的签名链识别号一致时(否则，直接得出验证失败的结论)，才进行后续的验证，如进行根据当前签名单元中的Hash值和本地签名单元中的Hash值计算待验证扩展值等动作。

[0062] 作为又一种实施方式，该度量请求还包括当前度量目标，也即，该度量请求包括当前度量目标和当前度量目标对应的当前签名单元，此时，在验证度量请求之前，先计算当前度量目标的Hash值，并验证当前签名单元中的Hash值与计算出的Hash值是否一致，只有在确定当前签名单元中的Hash值与计算出的Hash值一致时，才验证度量请求，否则，直接得出验证失败的结论。

[0063] 步骤S103：返回验证结果。

[0064] 返回验证通过(成功)或验证失败的验证结果，进而根据该验证结果决定是中止启动，还是继续启动。

[0065] 为了便于理解上述的度量请求的验证过程，下面以图4所示的交互图为例进行说明。其中，需要说明的是，图4所示的验证流程示意图仅是本申请众多实施例中的一种，因此不能将其理解成是对本申请的限制。

[0066] 其中，在根据当前签名单元验证当前度量目标的Hash值及签名值时，其过程可以为：安全处理器利用SM3算法计算当前度量目标的Hash值，对当前签名单元的签名值利用公钥进行解密得到解密后的值，验证计算出的Hash值、解密后的值和当前签名单元的度量目标的Hash值是否一致；若一致，则验证成功，否则，验证失败。

[0067] 其中，在根据当前签名单元和本地签名单元验证当前度量目标的hash值和签名值

时，其过程可以为：利用SM3算法计算当前度量目标的Hash值，验证计算出的Hash值与当前签名单元中的Hash值是否一致；在确定计算出的Hash值与当前签名单元中的Hash值一致时，根据当前签名单元中的Hash值和本地签名单元中的Hash值计算得到扩展值，利用公钥解密当前签名单元中的签名值，并验证计算的扩展值与解密后的签名值是否一致，若上述两个验证均一致，则验证成功，否则，验证失败。

[0068] 本申请通过签名链将各度量目标有机串联起来，启动时利用安全处理器对各度量目标严格按照签名链上的顺序依次进行完整性与依赖性双重度量，度量目标不可被绕过也不可被替换，保证了系统的整体完整性和一致性，进一步增强了系统启动安全。

[0069] 本申请实施例还提供了一种非易失性可读取存储介质(以下简称存储介质)，该存储介质上存储有可执行程序，该可执行程序被计算机如上述的计算机设备100执行时，执行上述的安全控制的方法。该存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0070] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0071] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

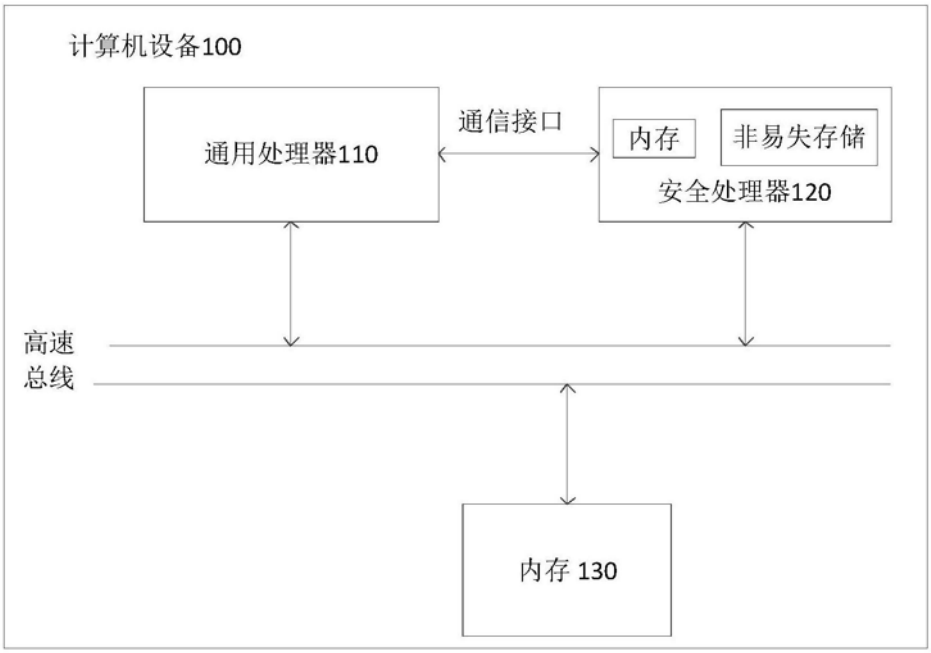

计算机设备100
通用处理器110
通信接口
内存
非易失存储
安全处理器120
高速
总线
内存 130

图1


签名单元0
签名单元1
签名单元2
签名单元n
签名值
签名链识别号
其他信息
度量目标
的Hash值

图2

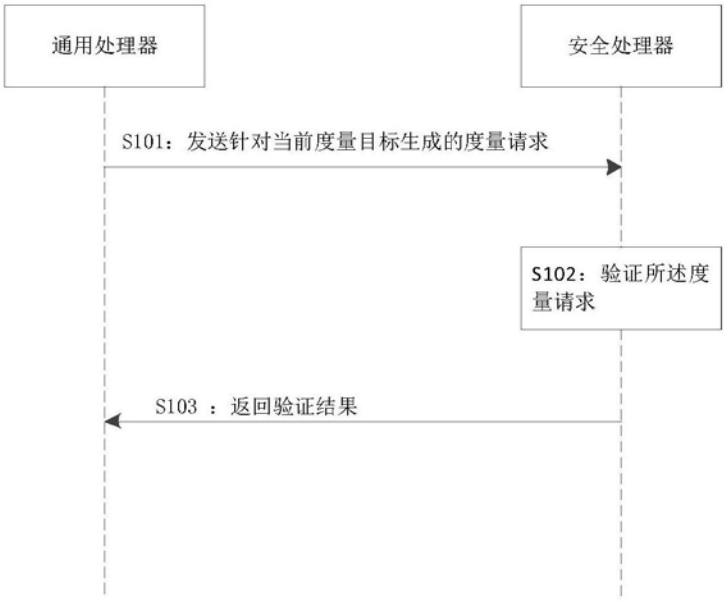

通用处理器
安全处理器
S101：发送针对当前度量目标生成的度量请求
S102：验证所述度量请求
S103 ：返回验证结果

图3

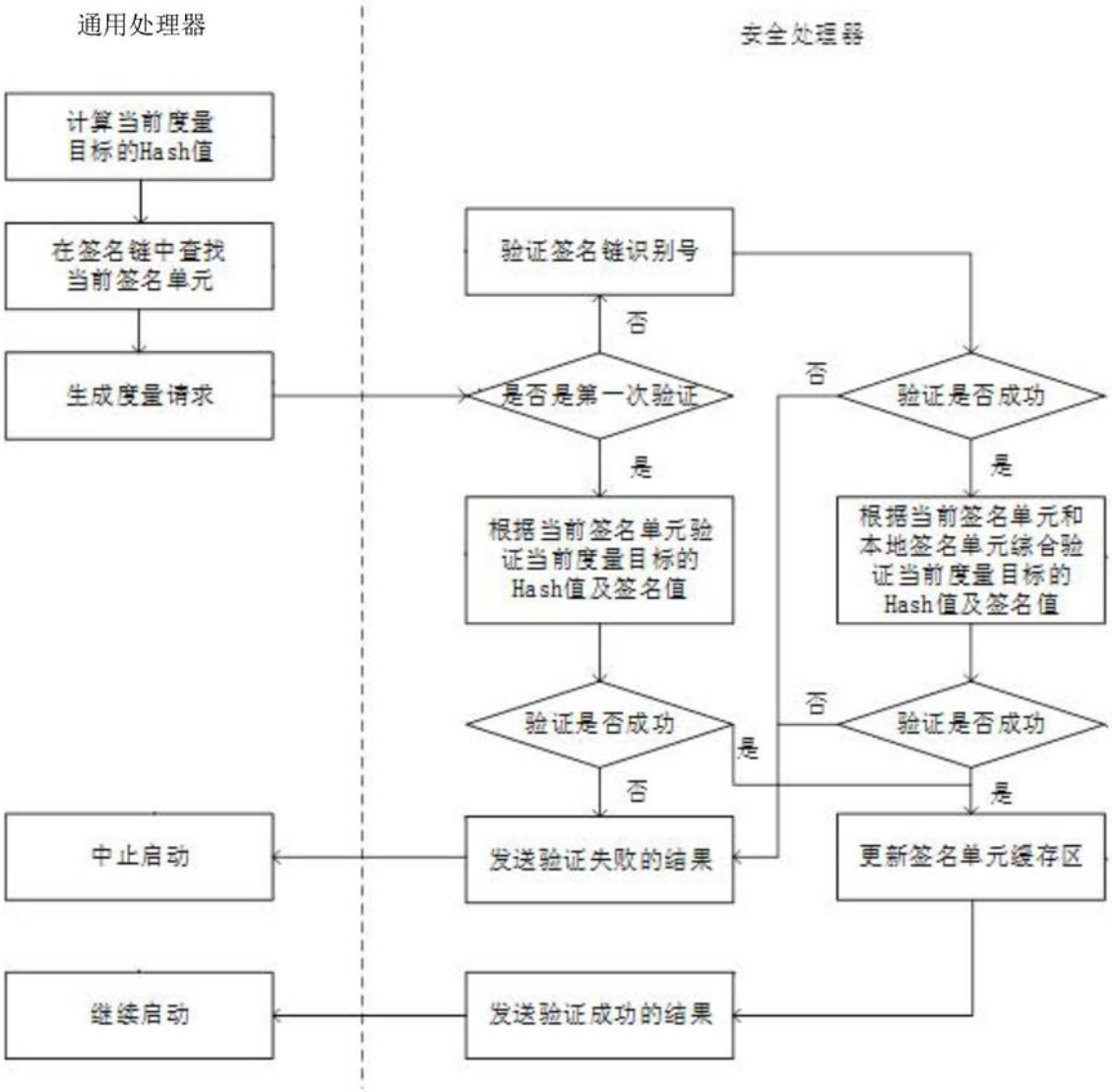

通用处理器
安全处理器
计算当前度量目标的Hash值
在签名链中查找当前签名单元
生成度量请求
验证签名链识别号
否
是否是第一次验证
是
根据当前签名单元验证当前度量目标的Hash值及签名值
验证是否成功
否
是
发送验证失败的结果
中止启动
否
验证是否成功
是
根据当前签名单元和本地签名单元综合验证当前度量目标的Hash值及签名值
验证是否成功
否
是
更新签名单元缓存区
发送验证成功的结果
继续启动

图4