(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113496011 B
(45)授权公告日 2024.01.26

(21)申请号 202010259146.3
(22)申请日 2020.04.03
(65)同一申请的已公布的文献号
申请公布号 CN 113496011 A
(43)申请公布日 2021.10.12
(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号
(72)发明人 郑一平
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
专利代理师 陈舒维 宋志强
(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/51(2013.01)
(56)对比文件
CN 108959943 A,2018.12.07
CN 110474767 A,2019.11.19
CN 110932853 A,2020.03.27
US 4817140 A,1989.03.28
审查员 孙国辉

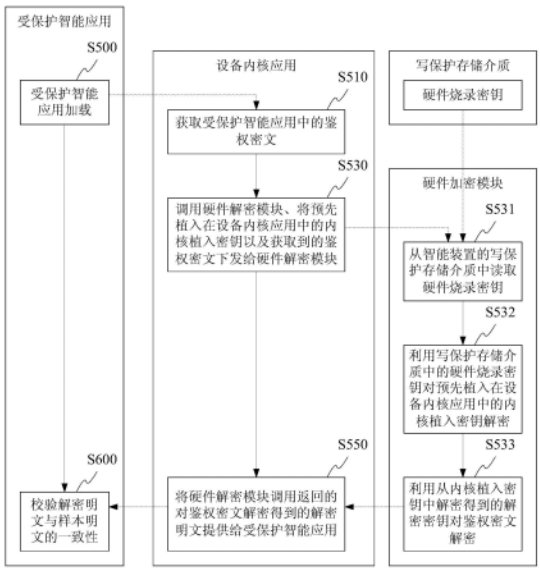
权利要求书2页 说明书8页 附图8页

(54)发明名称

受保护智能应用的调用权限认证方法以及智能装置

(57)摘要

本发明提供了受保护智能应用的调用权限认证方法以及智能装置。基于本发明,通过设备内核应用对硬件解密模块的调用,智能装置可以利用设备内核应用中的内核植入密钥、以及写保护存储介质中的硬件烧录密钥对受保护智能应用中的鉴权密文解密,只有当内核植入密钥为利用第一受管控密钥对第二受管控密钥加密得到的二级鉴权密钥、硬件烧录密钥为第一受管控密钥时,才能得到正确的第二受管控密钥对鉴权密文解密、并解密得到与样本明文一致的解密明文,以使受保护智能应用通过一致性验证、并对设备内核应用开放调用权限。从而,可以将受保护智能应用的使用权限制在具有正确密钥配置的智能装置,从而可以防御受保护智能应用在非法装置运行的恶意盗版行为。



CN 113496011 B

1.一种受保护智能应用的调用权限认证方法,其特征在于,当受保护智能应用被加载至智能装置时,该调用权限认证方法包括由智能装置的设备内核应用执行的如下步骤:

获取受保护智能应用中的鉴权密文;

调用硬件解密模块、并将预先植入在设备内核应用中的内核植入密钥以及获取到的鉴权密文下发给硬件解密模块,使硬件解密模块利用智能装置的写保护存储介质中的硬件烧录密钥对内核植入密钥解密、并利用从内核植入密钥中解密得到的解密密钥对鉴权密文解密;其中,当内核植入密钥为密钥服务器利用第一受管控密钥对第二受管控密钥加密得到的二级鉴权密钥、并且硬件烧录密钥为密钥服务器中的第一受管控密钥时,对内核植入密钥解密得到的解密密钥为密钥服务器使用的第二受管控密钥,并且,鉴权密文是利用对样本明文执行以二级鉴权密钥为输入密钥、并以第二受管控密钥为真实密钥对样本明文进行欺骗加密得到的;

将硬件解密模块调用返回的对鉴权密文解密得到的解密明文提供给受保护智能应用,以供受保护智能应用通过校验解密明文与样本明文的一致性来判决是否对设备内核应用开放调用权限;其中,当对内核植入密钥解密得到的解密密钥为第二受管控密钥时,对鉴权密文解密得到的解密明文与受保护智能应用中对设备内核应用访问屏蔽的样本明文一致。

2.根据权利要求1所述的调用权限认证方法,其特征在于,

二级鉴权密钥是利用第一受管控密钥对第二受管控密钥执行基于第一加密算法的加密操作而得到的;

鉴权密文是利用第二受管控密钥对样本明文执行基于第二加密算法的加密操作而得到的;

硬件解密模块利用硬件烧录密钥对内核植入密钥执行基于第一解密算法的解密操作,并且,硬件解密模块利用从内核植入密钥中解密得到的解密密钥对鉴权密文执行基于第二解密算法的解密操作;

其中,第一解密算法为第一加密算法的逆向算法,并且,第二解密算法为第二加密算法的逆向算法。

3.根据权利要求2所述的调用权限认证方法,其特征在于,鉴权密文是利用对样本明文执行基于第一解密算法的欺骗加密得到的,其中,该欺骗加密利用第一受管控密钥对输入密钥执行基于第一解密算法的解密操作、并以对输入密钥机密得到的欺骗密钥为真实密钥执行基于第二加密算法的加密操作。

4.根据权利要求1所述的调用权限认证方法,其特征在于,在受保护智能应用被加载至运行设备内核应用的智能装置之前,该调用权限认证方法进一步包括由智能装置的设备内核应用执行的如下步骤:

接收产线烧录设备提供的加密密钥数据;

对加密密钥数据执行解密操作;

利用从加密密钥数据中解密得到的密钥数据,在智能装置的写保护存储介质烧录形成硬件烧录密钥;其中,当产线烧录设备提供的加密密钥数据来自于密钥服务器时,从加密密钥数据中解密得到的密钥数据为第一受管控密钥;

在烧录完成后丢弃该密钥数据。

5.根据权利要求4所述的调用权限认证方法,其特征在于,产线烧录设备对密钥服务器

的访问权限,由插接在产线烧录设备的热插拔加密器件鉴权认证。

6.根据权利要求4所述的调用权限认证方法,其特征在于,接收烧录设备提供的加密密钥数据之前,进一步包括:

响应于产线烧录设备的认证检测,向产线烧录设备提供预先植入在设备内核应用中的认证信息。

7.根据权利要求1所述的调用权限认证方法,其特征在于,

第一受管控密钥的管控权归属于第一管理方;

第二受管控密钥的管控权归属于不同于第一管理方的第二管理方;

并且,第一管理方和第二管理方均不同于设备内核应用归属的第一开发方、以及受保护智能应用归属的第二开发方。

8.根据权利要求1所述的调用权限认证方法,其特征在于,智能装置的写保护存储介质为OTP存储介质。

9.一种智能装置,其特征在于,包括应用承载模块、硬件解密模块以及写保护存储介质,其中,应用承载模块用于加载运行设备内核应用,并且,当受保护智能应用被记载至应用承载模块时,设备内核应用用于执行如权利要求1至8中任一项所述的调用权限认证方法。

10.一种非瞬时计算机可读存储介质,其特征在于,所述非瞬时计算机可读存储介质存储指令,所述指令在由处理器执行时使得所述处理器加载设备内核应用、并引发设备内核应用执行如权利要求1至8中任一项所述的调用权限认证方法。

受保护智能应用的调用权限认证方法以及智能装置

技术领域

[0001] 本发明涉及智能应用的版权保护,特别涉及一种受保护智能应用的调用权限认证方法、以及应用该调用权限认证方法的智能装置。

背景技术

[0002] 随着智能化应用的广泛普及,各种智能应用也应运而生。然而,如何有效保护智能应用的版权使用,使智能应用的使用权能够被限制在指定授权范围内的智能装置,成为现有技术有待解决的技术问题。

发明内容

[0003] 有鉴于此,本发明的各实施例分别提供了一种受保护智能应用的调用权限认证方法、以及应用该调用权限认证方法的智能装置,有助于将受保护智能应用的使用权限制在指定授权范围内的智能装置。

[0004] 在一个实施例中,提供了一种受保护智能应用的调用权限认证方法,当受保护智能应用被加载至智能装置时,该调用权限认证方法包括由智能装置的设备内核应用执行的如下步骤:

[0005] 获取受保护智能应用中的鉴权密文;

[0006] 调用硬件解密模块、并将预先植入在设备内核应用中的内核植入密钥以及获取到的鉴权密文下发给硬件解密模块,使硬件解密模块利用智能装置的写保护存储介质中的硬件烧录密钥对内核植入密钥解密、并利用从内核植入密钥中解密得到的解密密钥对鉴权密文解密;其中,当内核植入密钥为密钥服务器利用第一受管控密钥对第二受管控密钥加密得到的二级鉴权密钥、并且硬件烧录密钥为密钥服务器中的第一受管控密钥时,对内核植入密钥解密得到的解密密钥为密钥服务器使用的第二受管控密钥,并且,鉴权密文是利用对样本明文执行以二级鉴权密钥为输入密钥、并以第二受管控密钥为真实密钥对样本明文进行欺骗加密得到的;

[0007] 将硬件解密模块调用返回的对鉴权密文解密得到的解密明文提供给受保护智能应用,以供受保护智能应用通过校验解密明文与样本明文的一致性来判决是否对设备内核应用开放调用权限;其中,当对内核植入密钥解密得到的解密密钥为第二受管控密钥时,对鉴权密文解密得到的解密明文与受保护智能应用中对设备内核应用访问屏蔽的样本明文一致。

[0008] 可选地,鉴权密文是利用对样本明文执行以二级鉴权密钥为输入密钥、并以第二受管控密钥为真实密钥的欺骗加密得到的。

[0009] 可选地,二级鉴权密钥是利用第一受管控密钥对第二受管控密钥执行基于第一加密算法的加密操作而得到的;鉴权密文是利用第二受管控密钥对样本明文执行基于第二加密算法的加密操作而得到的;硬件解密模块利用硬件烧录密钥对内核植入密钥执行基于第一解密算法的解密操作,并且,硬件解密模块利用从内核植入密钥中解密得到的解密密钥

对鉴权密文执行基于第二解密算法的解密操作;其中,第一解密算法为第一加密算法的逆向算法,并且,第二解密算法为第二加密算法的逆向算法。

[0010] 可选地,鉴权密文是利用对样本明文执行基于第一解密算法的欺骗加密得到的,其中,该欺骗加密利用第一受管控密钥对输入密钥执行基于第一解密算法的解密操作、并以对输入密钥机密得到的欺骗密钥为真实密钥执行基于第二加密算法的加密操作。

[0011] 可选地,在受保护智能应用被加载至运行设备内核应用的智能装置之前,该调用权限认证方法进一步包括由智能装置的设备内核应用执行的如下步骤:接收产线烧录设备提供的加密密钥数据;对加密密钥数据执行解密操作;利用从加密密钥数据中解密得到的密钥数据,在智能装置的写保护存储介质烧录形成硬件烧录密钥;其中,当产线烧录设备提供的加密密钥数据来自于密钥服务器时,从加密密钥数据中解密得到的密钥数据为第一受管控密钥;在烧录完成后丢弃该密钥数据。

[0012] 可选地,产线烧录设备对密钥服务器的访问权限,由插接在产线烧录设备的热插拔加密器件鉴权认证。

[0013] 可选地,接收烧录设备提供的加密密钥数据之前,进一步包括:响应于产线烧录设备的认证检测,向产线烧录设备提供预先植入在设备内核应用中的认证信息。

[0014] 可选地,第一受管控密钥的管控权归属于第一管理方;第二受管控密钥的管控权归属于不同于第一管理方的第二管理方;并且,第一管理方和第二管理方均不同于设备内核应用归属的第一开发方、以及受保护智能应用归属的第二开发方。

[0015] 可选地,智能装置的写保护存储介质为OTP存储介质。

[0016] 在另一个实施例中,提供了一种智能装置,包括应用承载模块、硬件解密模块以及写保护存储介质,其中,应用承载模块用于加载运行设备内核应用,并且,当受保护智能应用被记载至应用承载模块时,设备内核应用用于执行如前述实施例所述的调用权限认证方法。

[0017] 在另一个实施例中,提供了一种非瞬时计算机可读存储介质,所述非瞬时计算机可读存储介质存储指令,所述指令在由处理器执行时使得所述处理器加载设备内核应用、并引发设备内核应用执行如述实施例所述的调用权限认证方法。

[0018] 基于上述实施例,通过设备内核应用对硬件解密模块的调用,智能装置可以利用设备内核应用中的内核植入密钥、以及写保护存储介质中的硬件烧录密钥对受保护智能应用中的鉴权密文解密,并且,只有当内核植入密钥为利用第一受管控密钥对第二受管控密钥加密得到的二级鉴权密钥、硬件烧录密钥为第一受管控密钥时,才能得到正确的第二受管控密钥对鉴权密文解密、并解密得到与样本明文一致的解密明文,以使受保护智能应用通过一致性验证而对设备内核应用开放调用权限。从而,可以将受保护智能应用的使用权限制在正确配置有二级鉴权密钥、并烧录有第一受管控密钥的智能装置,从而可以防御受保护智能应用在非法装置运行的恶意盗版行为。

附图说明

[0019] 以下附图仅对本发明做示意性说明和解释,并不限定本发明的范围:

[0020] 图1为一个实施例中的密钥合法部署方案的原理性示意图;

[0021] 图2为如图1所示的密钥合法部署方案的实例流程示意图;

[0022] 图3为如图1所示的密钥合法部署方案的优化原理示意图;

[0023] 图4为如图3所示的密钥合法部署方案的实例流程示意图;

[0024] 图5为一个实施例中的受保护智能应用的调用权限认证方法的示例性流程示意图;

[0025] 图6为如图5所示的调用权限认证方法可以防御的密钥非法部署行为的示意图;

[0026] 图7为如图5所示的调用权限认证方法的实例化流程示意图;

[0027] 图8为如图5所示的调用权限认证方法支持如图2所示密钥合法部署实例的扩展流程示意图;

[0028] 图9为一个实施例中的智能装置的示例性结构示意图。

具体实施方式

[0029] 为了使本发明的目的、技术方案及优点更加清楚明白,以下参照附图并举实施例,对本发明作进一步详细说明。

[0030] 图1为一个实施例中的密钥合法部署方案的示意图。请参见图1,为了实现受保护智能应用(例如智能算法库)在指定授权范围内的智能装置(例如智能卡)的加载运行,该实施例中的密钥合法部署方案提供了三种密钥,分别为第一受管控密钥Key_root 110(也可以称为根密钥)、第二受管控密钥Key_alg 120(也可以称为智能应用原始密钥)、以及二级鉴权密钥Key_ladder 130(也可以称为工作密钥)。

[0031] 第一受管控密钥Key_root 110可以为AES(Advanced Encryption Standard,高级加密标准)密钥;第一受管控密钥Key_root 110可以作为智能装置200中合法的硬件烧录密钥烧录在智能装置200的写保护存储介质220中,该写保护存储介质220可以为例如OTP(One Time Programmable,一次可编程)存储介质等能够防御硬件烧录密钥被篡改的介质;并且,第一受管控密钥Key_root 110的管控权归属于第一管理方510,该第一管理方510不同于设备内核应用210归属的第一开发方410、以及受保护智能应用300归属的第二开发方420。为了便于第一受管控密钥Key_root 110对第一开发方410和第二开发方420的保密隔离,第一受管控密钥Key_root 110可以借助受访问权限控制的密钥服务器100作为中转载体。

[0032] 第二受管控密钥Key_alg 120也可以为AES密钥,第二受管控密钥Key_alg 120可以作为加密得到受保护智能应用中的密文的合法加密密钥,并且,第二受管控密钥Key_alg 120的管控权归属于第二管理方520,该第二管理方520既不同于第一管理方510,也不同于设备内核应用210归属的第一开发方410、以及受保护智能应用300归属的第二开发方420。

[0033] 二级鉴权密钥Key_ladder 130可以为基于密钥分级(Key Ladder)机制,利用第一受管控密钥Key_root 110对第二受管控密钥Key_alg 120加密得到的二级密钥。二级鉴权密钥Key_ladder 130可以在设备内核应用210归属的第一开发方410群组共享,并且,二级鉴权密钥Key_ladder 130可以作为内核植入密钥而被第一开发方410植入在设备内核应用210中。

[0034] 图2为如图1所示的密钥合法部署方案的实例流程示意图。请参见图2,在一个密钥合法部署实例中:

[0035] 第一开发方410(例如设备内核应用的归属方的开发组)可以在密钥服务器100部署密钥分派工具(S411),其中,密钥分派工具在密钥服务器100的部署位置可以仅对第一开

发方410可知。

[0036] 当密钥服务器100成功完成密钥分派工具的安装(S101)后,第一开发方410会收到密钥服务器100返回的成功响应(S102),此时,密钥服务器100具备了作为第一受管控密钥Key_root 110的中转载体的能力。

[0037] 第一管控方510(例如设备内核应用的归属方的密钥管理员)可以将第一受管控密钥Key_root 110上传至密钥服务器100(S511),以供密钥服务器100在本地存储第一受管控密钥Key_root 110(S103)。其中,第一受管控密钥Key_root 110在密钥服务器100的存储位置可以由第一管控方510指定、并且仅对第一管控方510可知。

[0038] 第二管控方520(例如受保护智能应用的归属方的密钥管理员)可以将第二受管控密钥Key_alg 120上传至密钥服务器100(S521),以供密钥服务器100调用部署的密钥分派工具、并利用本地存储第一受管控密钥Key_root 110对上传的第二受管控密钥Key_alg 120加密,得到基于分级加密机制的二级鉴权密钥Key_ladder 130(S104)。

[0039] 此后,密钥服务器100可以将基于分级加密机制的二级鉴权密钥Key_ladder130下发至第一开发方410(S105),从而,第一开发方410即可留存二级鉴权密钥Key_ladder 130、并将二级鉴权密钥Key_ladder 130植入设备内核应用中(S412),再将植入了二级鉴权密钥Key_ladder 130的设备内核应用交由产线固化加载于智能装置200(S413)。

[0040] 固化加载有设备内核应用的智能装置200将会在产线继续执行后续工序,其中包括利用产线烧录设备430的硬件烧录密钥的烧录过程,即,产线烧录设备430可以发起对智能装置200的认证检测(S431),智能装置200中的设备内核应用可以响应于产线烧录设备430的认证检测,向产线烧录设备430提供预先植入在设备内核应用中的认证信息(S201)。

[0041] 当产线烧录设备430根据认证信息检测出智能装置200为合法且版本正确的装置时,其可以向密钥服务器100发起密钥请求(S432)。其中,产线烧录设备430对密钥服务器100的访问权限,可以由插接在产线烧录设备430的热插拔加密器件(例如加密狗)鉴权认证,从而,密钥服务器100在接收到密钥请求、并且对密钥请求鉴权认证通过后,会向产线烧录设备430下发加密的密钥数据(S106)。

[0042] 产线烧录设备430并不具备对密钥数据的解密能力,因此,产线烧录设备430会将加密的密钥数据转发至智能装置200(S433)。

[0043] 智能装置200的设备内核应用接收到产线烧录设备430提供的加密密钥数据,可以按照与密钥服务器100使用的加密算法(例如混淆算法)的逆向算法(例如解混淆算法),对加密密钥数据执行解密操作(S202),并利用从加密密钥数据中解密得到的密钥数据(此时为第一受管控密钥Key_root 110),在智能装置200的写保护存储介(例如OTP存储介质)质烧录形成硬件烧录密钥(S203),烧录完成后,智能装置200的设备内核应用可以丢弃烧录时使用的密钥数据。

[0044] 第二开发方420(例如受保护智能应用的归属方的开发组)可以将鉴权明文提供给第二管控方520(S421)进行基于第二受管控密钥Key_alg 120的加密(S522),在接收到第二管控方520提供的鉴权密文(S523)后,第二开发方420即可将加权密文和鉴权明文植入在受保护智能应用中(S422),其中,鉴权密文在受保护智能应用中以访问不受限的方式植入、而鉴权明文则以对设备内核应用屏蔽访问的方式植入。

[0045] 图3为如图1所示的密钥合法部署方案的优化原理示意图。图4为如图3所示的密钥

合法部署方案的实例流程示意图。作为一种扩展方式,基于对鉴权明文加密的鉴权密文产生过程,也可以在第二开发方420完成,例如,密钥服务器100也可以将二级鉴权密钥Key_ladder 130分别下发至第二管控方520(S107)和第二开发方420(S108)留存。

[0046] 第二管控方520可以制作用于实现欺骗加密的明文加密工具(S522)并提供给第二开发方420(S523),该欺骗加密以二级鉴权密钥Key_ladder 130为输入密钥、并以第二受管控密钥Key_alg 120为真实密钥执行加密操作。

[0047] 从而,第二开发方420可以利用留存的二级鉴权密钥Key_ladder 130,利用第二管控方520提供的明文加密工具实现对鉴权明文的加密(S421'),得到以第二受管控密钥Key_alg 120为真实密钥执行加密的鉴权密文,此后,第二开发方420即可将加权密文和鉴权明文植入在受保护智能应用中(S422),其中,鉴权密文在受保护智能应用中以访问不受限的方式植入、而鉴权明文则以对设备内核应用屏蔽访问的方式植入。

[0048] 以上对密钥合法部署的说明,旨在便于理解第一受管控密钥Key_root 110(也可以称为根密钥)用于在智能装置烧录、第二受管控密钥Key_alg 120(也可以称为智能应用原始密钥)用于产生受保护智能应用的鉴权密文、以及二级鉴权密钥Key_ladder 130用于触发解密认证或进一步用于触发密文加密的密钥关系,可以理解的是,上述密钥合法部署中的操作流程、各方身份、以及密钥分派细节,不应当构成对密钥关系的必要限制。

[0049] 在下文中,将结合具有上述密钥关系第一受管控密钥Key_root 110、第二受管控密钥Key_alg 120、以及二级鉴权密钥Key_ladder 130,对受保护智能应用的调用权限认证方法进行详细说明。

[0050] 图5为一个实施例中的受保护智能应用的调用权限认证方法的示例性流程示意图。请参见图5,在受保护智能应用被加载至智能装置(S500)时,该实施例中的受保护智能应用的调用权限认证方法可以包括由智能装置的设备内核应用执行的如下步骤:

[0051] S510:获取受保护智能应用中的鉴权密文。

[0052] S530:调用硬件解密模块、并将预先植入在设备内核应用中的内核植入密钥以及获取到的鉴权密文下发给硬件解密模块,使硬件解密模块:

[0053] 在S53 1从智能装置的写保护存储介质中读取硬件烧录密钥;

[0054] 在S533利用写保护存储介质中的硬件烧录密钥对预先植入在设备内核应用中的内核植入密钥解密;以及

[0055] 在S535利用从内核植入密钥中解密得到的解密密钥对鉴权密文解密。

[0056] 例如,二级鉴权密钥Key_ladder可以是利用第一受管控密钥Key_root对第二受管控密钥Key_a|g执行基于第一加密算法的加密操作而得到的,鉴权密文是利用第二受管控密钥Key_alg对样本明文加密得到的,相应地,硬件解密模块可以利用硬件烧录密钥对内核植入密钥执行基于第一解密算法(第一加密算法的逆向算法)的解密操作,并且,硬件解密模块利用从内核植入密钥中解密得到的解密密钥对鉴权密文执行基于第二解密算法(第二加密算法的逆向算法)的解密操作;

[0057] 从而,当内核植入密钥为利用第一受管控密钥Key_root对第二受管控密钥Key_alg加密得到的二级鉴权密钥Key_ladder、并且硬件烧录密钥为第一受管控密钥Key_root时,对内核植入密钥解密得到的解密密钥为第二受管控密钥Key_alg。

[0058] 若鉴权密文是利用对样本明文执行以二级鉴权密钥Key_ladder为输入密钥、并以

第二受管控密钥Key_alg为真实密钥的欺骗加密得到的,则,该欺骗加密利用可以第一受管控密钥Key_root对输入密钥执行基于第一解密算法(第一加密算法的逆向算法)的解密操作、并以对输入密钥机密得到的欺骗密钥(第二受管控密钥Key_alg)为真实密钥执行基于第二加密算法的加密操作。

[0059] S550:将硬件解密模块调用返回的对鉴权密文解密得到的解密明文提供给受保护智能应用,以供受保护智能应用在S600通过校验解密明文与样本明文的一致性来判决是否对设备内核应用开放调用权限。

[0060] 其中,当对内核植入密钥解密得到的解密密钥为第二受管控密钥Key_alg时,对鉴权密文解密得到的解密明文与受保护智能应用中对设备内核应用访问屏蔽的样本明文一致。

[0061] 基于上述流程,通过设备内核应用对硬件解密模块的调用,智能装置可以利用设备内核应用中的内核植入密钥、以及写保护存储介质中的硬件烧录密钥对受保护智能应用中的鉴权密文解密,并且:

[0062] 只有当内核植入密钥为利用第一受管控密钥Key_root对第二受管控密钥Key_alg加密得到的二级鉴权密钥Key_ladder、硬件烧录密钥为第一受管控密钥Key_root时,才能得到正确的第二受管控密钥Key_alg对鉴权密文解密、并解密得到与样本明文一致的解密明文,以使受保护智能应用通过一致性验证而对设备内核应用开放调用权限。

[0063] 从而,可以将受保护智能应用的使用权限制在正确配置有二级鉴权密钥Key_ladder、并烧录有第一受管控密钥Key_root的智能装置,从而可以防御受保护智能应用在非法装置运行的恶意盗版行为。

[0064] 图6为如图1所示的调用权限认证方法可以防御的密钥非法部署行为的示意图。请参见图6,若有盗版者610仿制智能装置的硬件及其加载的设备内核应用,则,盗版者610难以同时获得二级鉴权密钥Key_ladder和第一受管控密钥Key_root,从而,导致仿冒智能装置不能获得受保护应用300的调用权限。

[0065] 图7为如图5所示的调用权限认证方法的实例化流程示意图。请参见图7,受保护智能应用中包括智能应用内核310、应用校验模块320、对设备内核应用开放访问权限的访问接口331和校验接口332、以及对设备内核应用提供受限访问权限的调用接口390。

[0066] 其中,访问接口331和校验接口332以及调用接口390都可以为API(Application Programming Interface,应用程序接口),并且,以访问不受限的方式植入在受保护智能应用中的鉴权密文可以集成在访问接口331中,以对设备内核应用屏蔽访问的方式植入在受保护智能应用中的鉴权明文可以隐藏集成在用用校验模块320中。

[0067] 相应地,在图7中,设备内核应用可以在S510通过读取受保护智能应用的访问接口331来获取鉴权密文,并且,设备内核应用可以在S550将解密明文发送至校验接口332,以供受保护智能应用中的应用校验模块320校验解密明文与样本明文的一致性、并以此来判决是否对设备内核应用开放调用权限。

[0068] 另外,在图7中,调用权限认证方法可以在S550之后,进一步包括由设备内核应用执行的S570:接收受保护智能应用(应用校验模块320)返回的校验结果,并通过识别校验结果来判断,是否有权调用受保护智能应用,即,是否可以通过访问调用接口390而得到对智能应用内核310的成功调用响应。

[0069] 图8为如图5所示的调用权限认证方法支持如图2所示密钥合法部署实例的扩展流程示意图。请参见图8,在受保护智能应用被加载至智能装置之前(例如智能装置处于产线制造阶段),该实施例中的受保护智能应用的调用权限认证方法可以包括由智能装置的设备内核应用执行的如下步骤:

[0070] S810:接收产线烧录设备提供的加密密钥数据。

[0071] S830:对加密密钥数据执行解密操作。

[0072] S850:利用从加密密钥数据中解密得到的密钥数据,在智能装置的写保护存储介质烧录形成硬件烧录密钥。

[0073] 其中,当产线烧录设备提供的加密密钥数据来自于密钥服务器时,从加密密钥数据中解密得到的密钥数据为第一受管控密钥Key_root。

[0074] 并且,作为进一步可选的优化方案,产线烧录设备对密钥服务器的访问权限,可以由插接在产线烧录设备的热插拔加密器件(例如加密狗)鉴权认证。

[0075] S870:在烧录完成后丢弃该密钥数据。

[0076] 另外,作为进一步的可选方案,在S810之前,该实施例中的受保护智能应用的调用权限认证方法可以包括由智能装置的设备内核应用执行的步骤:响应于产线烧录设备的认证检测,向产线烧录设备提供预先植入在设备内核应用中的认证信息。

[0077] 图9为一个实施例中的智能装置的示例性结构示意图。请参见图9,在该实施例中,智能装置(其可以呈现为智能卡的形态)包括应用承载模块910、硬件解密模块920以及写保护存储介质930(例如OTP存储介质)。

[0078] 应用承载模块910用于加载运行设备内核应用,并且,当受保护智能应用被记载至应用承载模块时,设备内核应用用于执行如前述实施例所述的调用权限认证方法,即,执行如图5或图7所示的流程,还可以进一步执行如图8所示的流程。

[0079] 硬件解密模块920用于为应用承载模块910中加载的设备内核应用提供解密辅助,即,执行如图5或图7所示流程中的S531、S533以及S535中的步骤。

[0080] 写保护存储介质930中烧录有硬件烧录密钥,例如,硬件烧录密钥可以通过如图8所示的流程烧录在该写保护存储介质930中。

[0081] 在实现上述智能装置时,应用承载模块910、硬件解密模块920以及写保护存储介质930(例如OTP存储介质)可以集成在同一块IC(Integrated Circuit,集成电路)芯片中。

[0082] 智能装置还可以进一步包括非瞬时计算机可读存储介质,该非瞬时计算机可读存储介质可以独立于集成有应用承载模块910、硬件解密模块920以及写保护存储介质930的IC芯片,并且,非瞬时计算机可读存储介质中可以存储指令,其中一部分指令在由例如该IC芯片等处理器执行时,可以使得例如该IC芯片等处理器加载设备内核应用(加载至应用承载模块910)、并引发设备内核应用如前述实施例所述的调用权限认证方法,即,执行如图5或图7所示的流程,还可以进一步执行如图8所示的流程。

[0083] 该非瞬时计算机可读存储介质中还可导入用于例如该IC芯片等处理器加载受保护智能应用(加载至应用承载模块910)的另一些指令。

[0084] 硬件解密模块920实现解密过程的算法,可以预先固化在硬件解密模块920中,而不通过从非瞬时计算机可读存储介质加载程序的方式实现。

[0085] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精

神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明保护的范围之内。

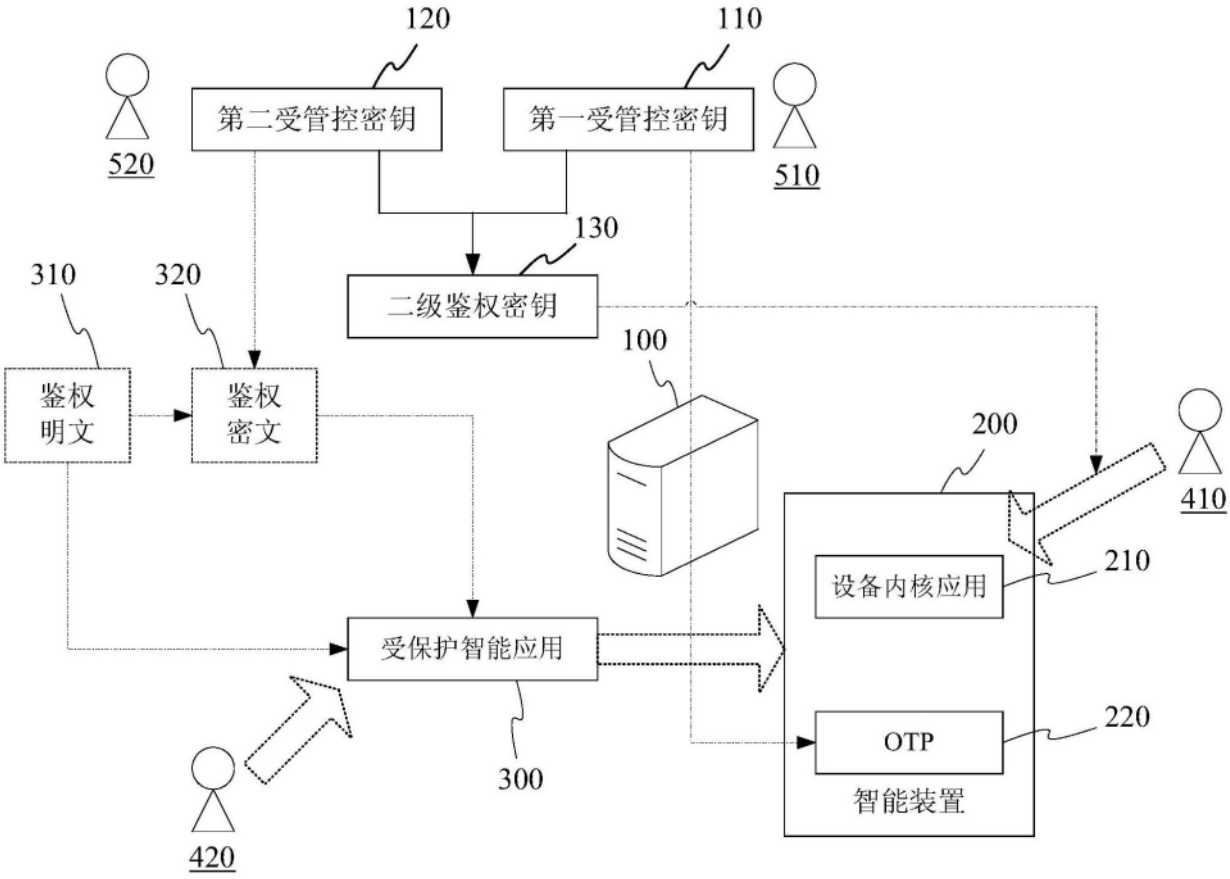

120
110
第二受管控密钥
第一受管控密钥
520
510
130
310
320
二级鉴权密钥
100
鉴权
明文
鉴权
密文
200
410
设备内核应用
210
受保护智能应用
OTP
220
300
智能装置
420

图1

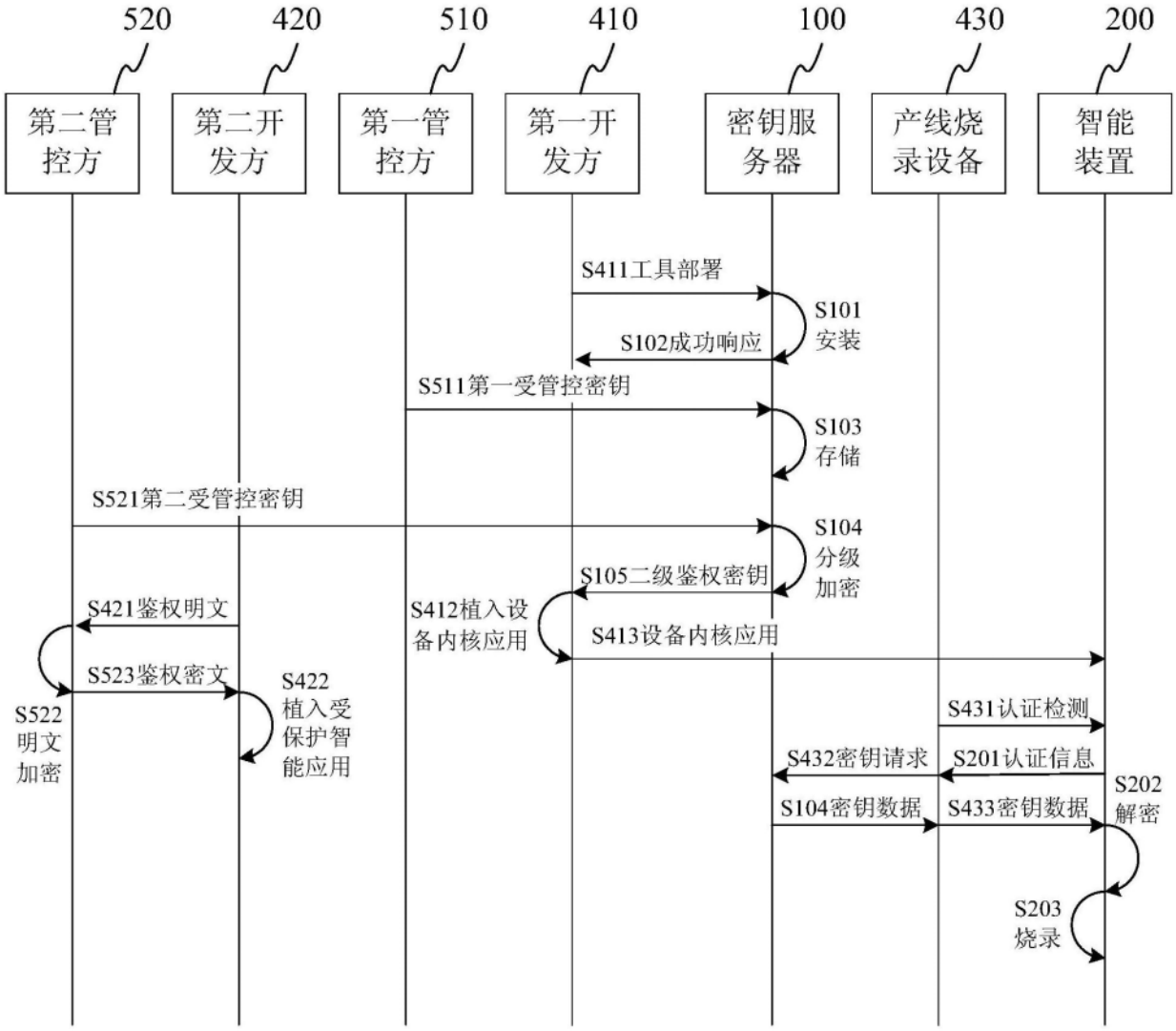

520
420
510
410
100
430
200
第二管控方
第二开发方
第一管控方
第一开发方
密钥服务器
产线烧录设备
智能装置
S411工具部署
S101安装
S102成功响应
S511第一受管控密钥
S103存储
S521第二受管控密钥
S104分级加密
S105二级鉴权密钥
S421鉴权明文
S412植入设备内核应用
S413设备内核应用
S523鉴权密文
S422植入受保护智能应用
S522明文加密
S431认证检测
S432密钥请求
S201认证信息
S202解密
S104密钥数据
S433密钥数据
S203烧录

图2

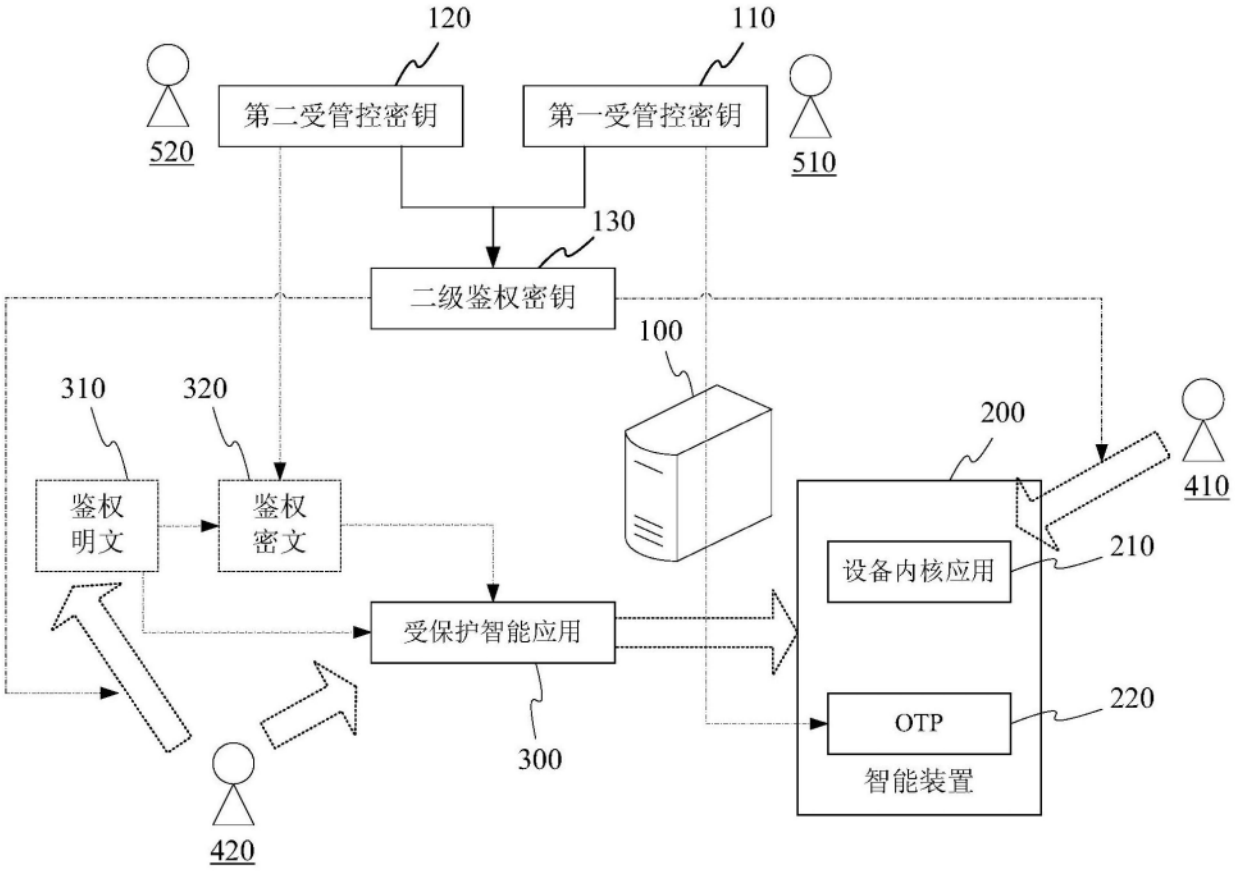

120
110
第二受管控密钥
第一受管控密钥
520
510
130
二级鉴权密钥
100
310
320
200
410
鉴权
明文
鉴权
密文
设备内核应用
210
受保护智能应用
OTP
220
300
智能装置
420

图3

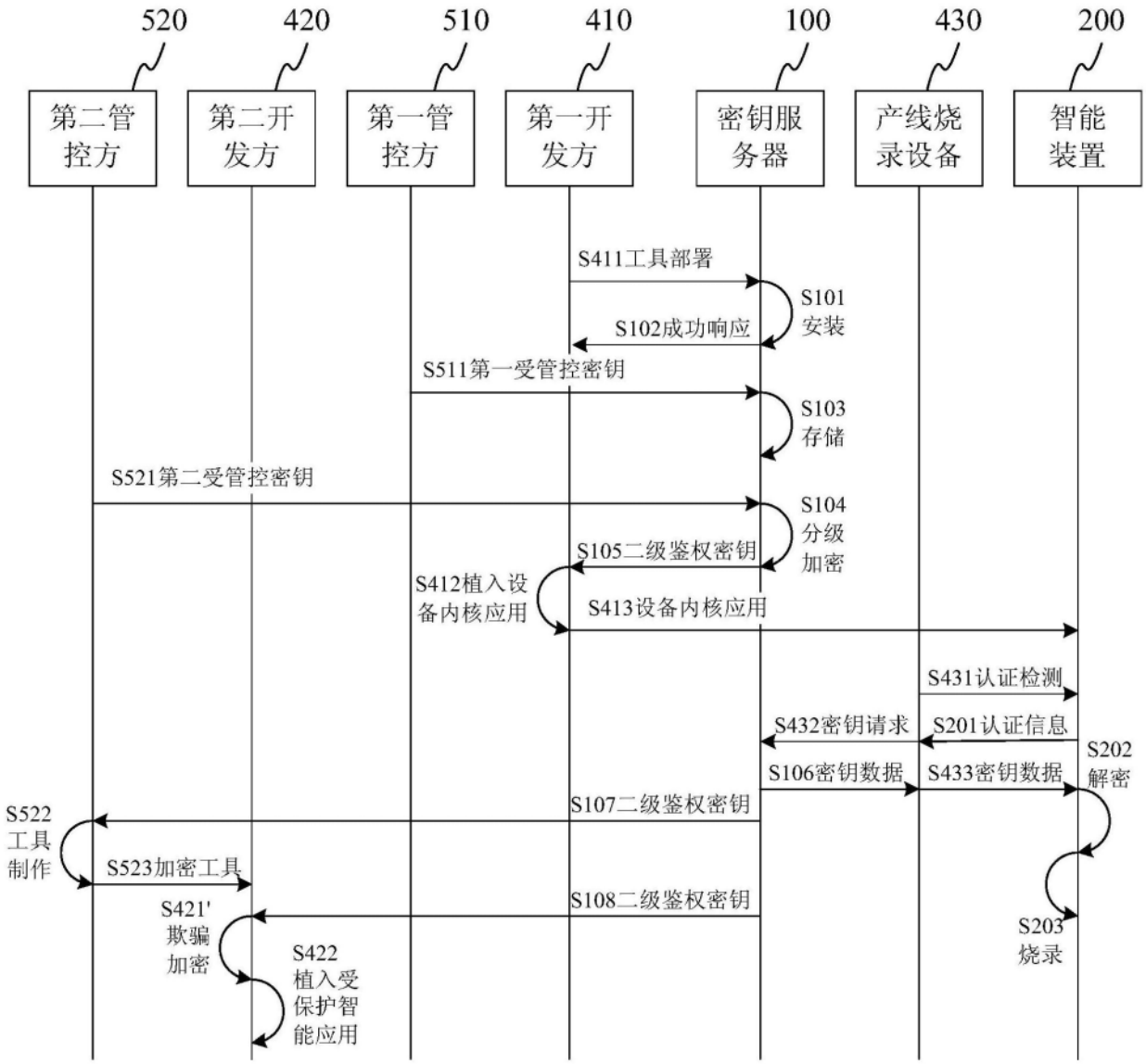

520
420
510
410
100
430
200
第二管控方
第二开发方
第一管控方
第一开发方
密钥服务器
产线烧录设备
智能装置
S411工具部署
S101安装
S102成功响应
S511第一受管控密钥
S103存储
S521第二受管控密钥
S104分级加密
S105二级鉴权密钥
S412植入设备内核应用
S413设备内核应用
S431认证检测
S432密钥请求
S201认证信息
S202解密
S106密钥数据
S433密钥数据
S107二级鉴权密钥
S522工具制作
S523加密工具
S108二级鉴权密钥
S421'欺骗加密
S422植入受保护智能应用
S203烧录

图4

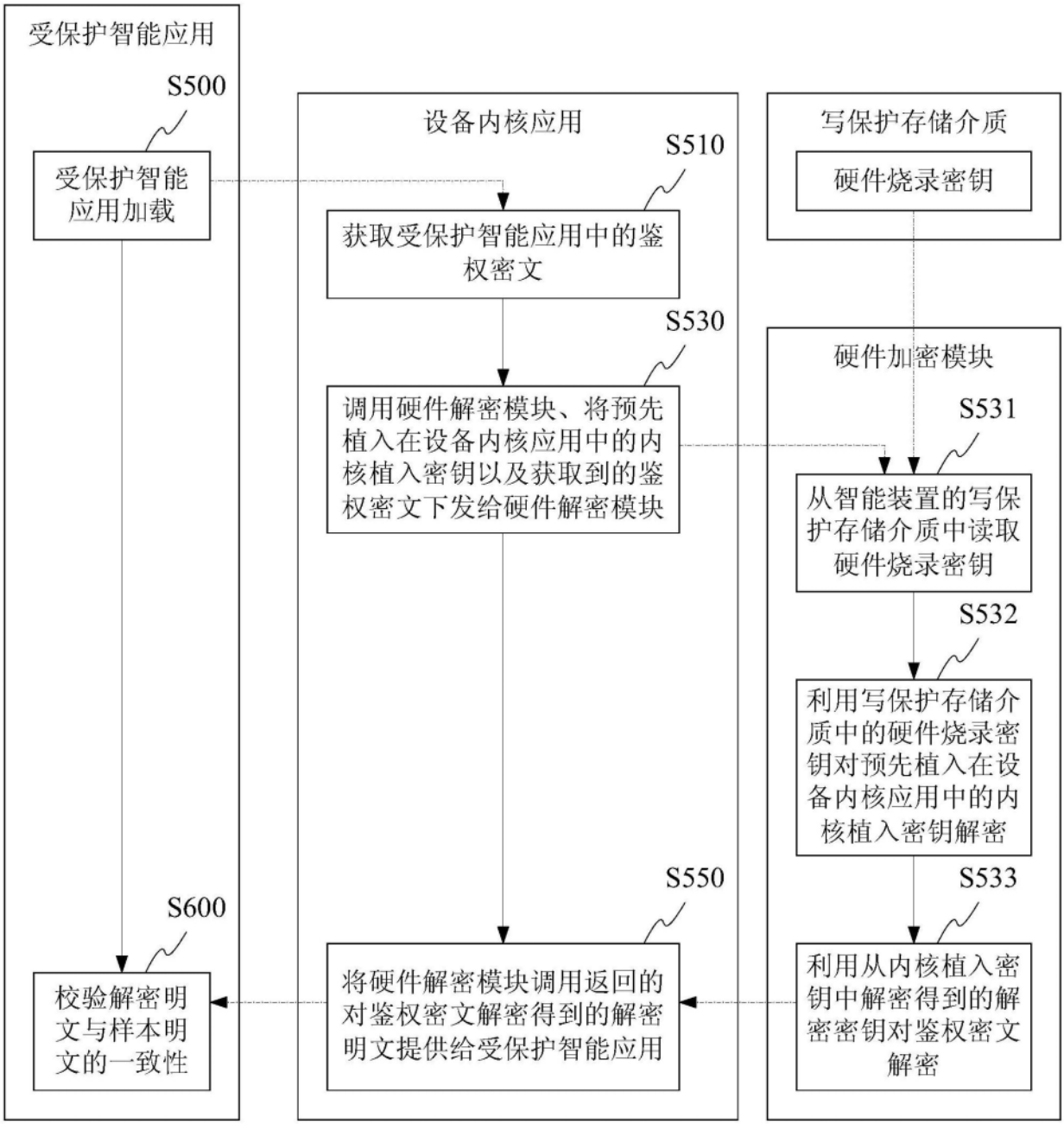

受保护智能应用
S500
受保护智能应用加载
S600
校验解密明文与样本明文的一致性
设备内核应用
S510
获取受保护智能应用中的鉴权密文
S530
调用硬件解密模块、将预先植入在设备内核应用中的内核植入密钥以及获取到的鉴权密文下发给硬件解密模块
S550
将硬件解密模块调用返回的对鉴权密文解密得到的解密明文提供给受保护智能应用
写保护存储介质
硬件烧录密钥
硬件加密模块
S531
从智能装置的写保护存储介质中读取硬件烧录密钥
S532
利用写保护存储介质中的硬件烧录密钥对预先植入在设备内核应用中的内核植入密钥解密
S533
利用从内核植入密钥中解密得到的解密密钥对鉴权密文解密

图5

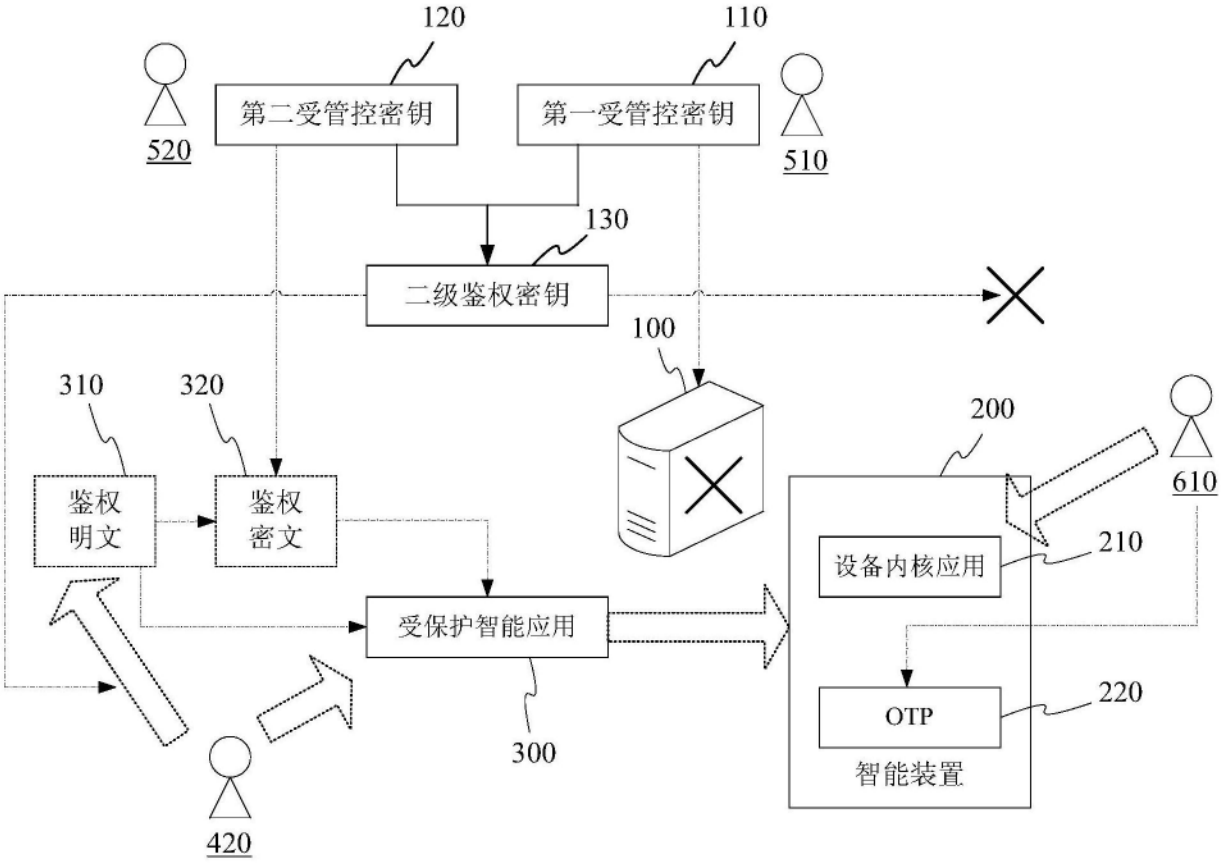

120
110
第二受管控密钥
第一受管控密钥
520
510
130
二级鉴权密钥
100
310
320
200
610
鉴权
明文
鉴权
密文
设备内核应用
210
受保护智能应用
OTP
220
300
智能装置
420

图6

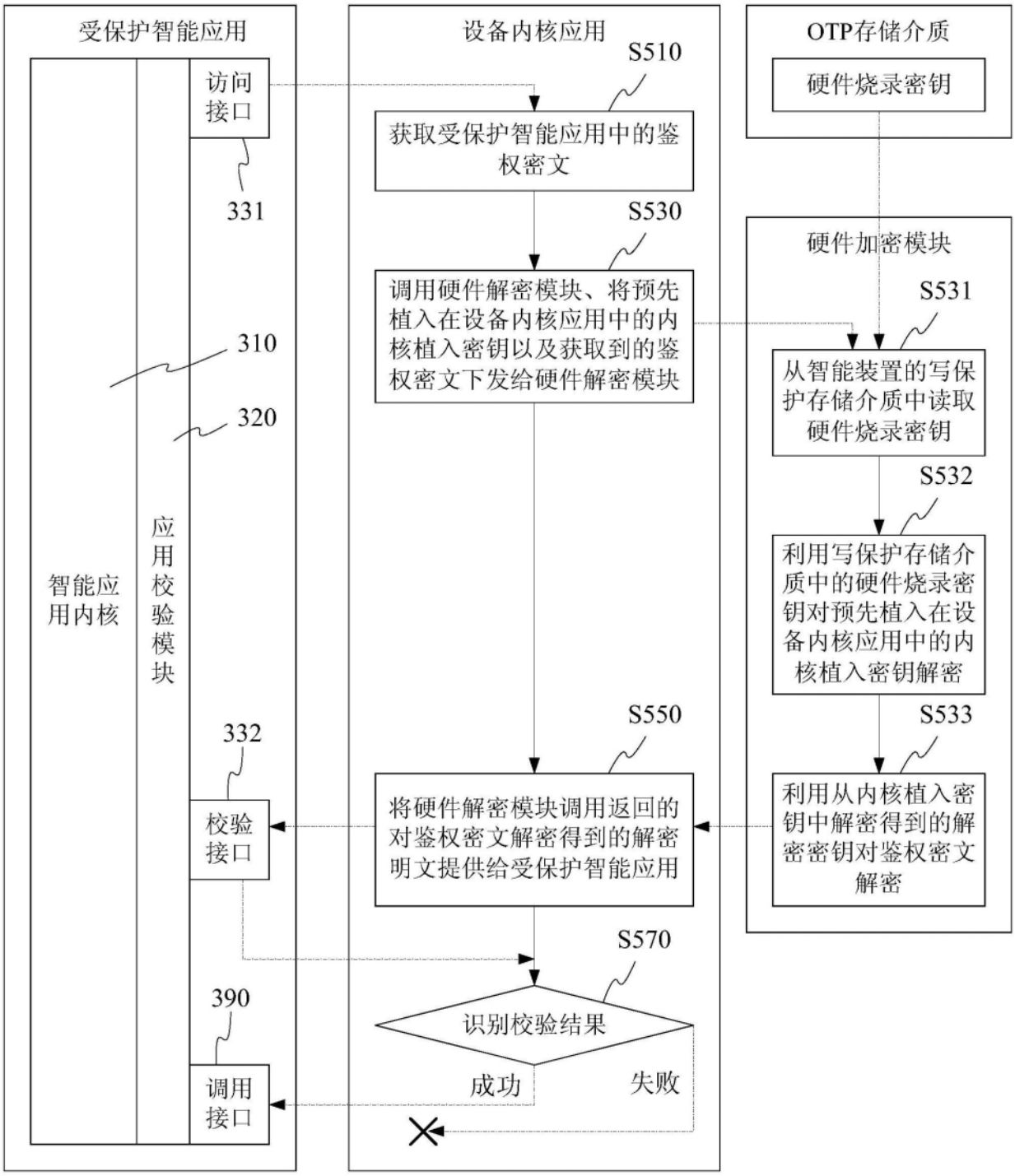

受保护智能应用
访问接口
331
310
320
智能应用内核
应用校验模块
332
校验接口
390
调用接口
设备内核应用
S510
获取受保护智能应用中的鉴权密文
S530
调用硬件解密模块、将预先植入在设备内核应用中的内核植入密钥以及获取到的鉴权密文下发给硬件解密模块
S550
将硬件解密模块调用返回的对鉴权密文解密得到的解密明文提供给受保护智能应用
S570
识别校验结果
成功
失败
OTP存储介质
硬件烧录密钥
硬件加密模块
S531
从智能装置的写保护存储介质中读取硬件烧录密钥
S532
利用写保护存储介质中的硬件烧录密钥对预先植入在设备内核应用中的内核植入密钥解密
S533
利用从内核植入密钥中解密得到的解密密钥对鉴权密文解密

图7

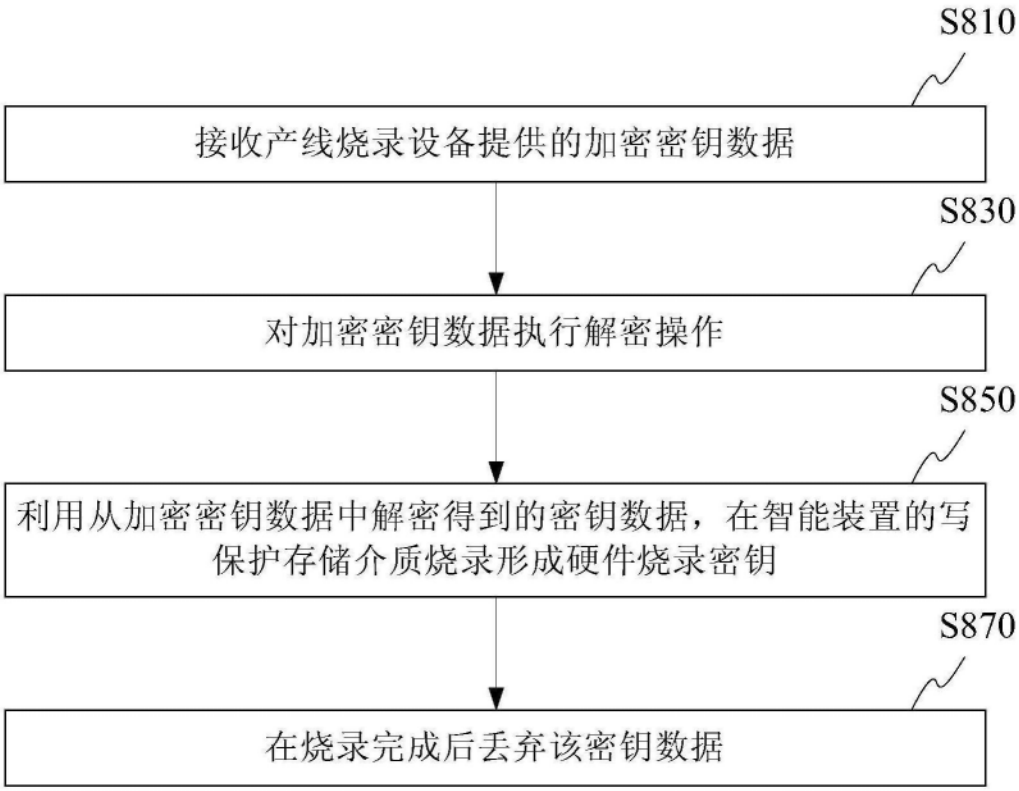

S810
接收产线烧录设备提供的加密密钥数据
S830
对加密密钥数据执行解密操作
S850
利用从加密密钥数据中解密得到的密钥数据，在智能装置的写保护存储介质烧录形成硬件烧录密钥
S870
在烧录完成后丢弃该密钥数据

图8

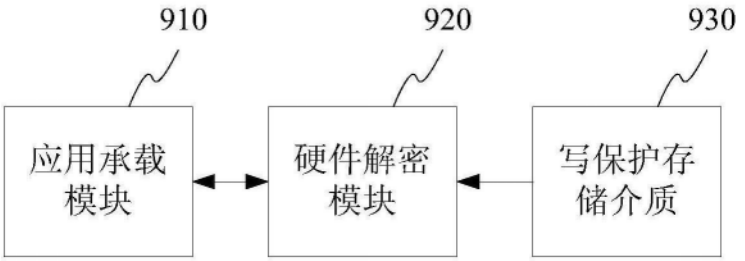

910
920
930
应用承载模块
硬件解密模块
写保护存储介质

图9