

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 10 月 4 日 (04.10.2018)



(10) 国际公布号
WO 2018/176707 A1

(51) 国际专利分类号:
G06F 9/445 (2006.01)

(21) 国际申请号: PCT/CN2017/095333

(22) 国际申请日: 2017 年 7 月 31 日 (31.07.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710208114.9 2017年3月31日 (31.03.2017) CN

(71) 申请人: 深圳市中兴微电子有限公司
(**SANECIPS TECHNOLOGY CO., LTD.**) [CN/CN];
中国广东省深圳市南山区西丽街道留仙大道
中兴工业园, Guangdong 518055 (CN)。

(72) 发明人: 韩宏娜 (**HAN, Hongna**); 中国广东省深圳
市南山区西丽街道留仙大道中兴工业
园, Guangdong 518055 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司
(**CHINA PAT INTELLECTUAL PROPERTY
OFFICE**); 中国北京市海淀区海淀南路21号中关村
知识产权大厦B座2层, Beijing 100080 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家
保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,
CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,
LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(54) **Title:** METHOD AND DEVICE FOR STARTING EMBEDDED SYSTEM, AND COMPUTER STORAGE MEDIUM

(54) 发明名称: 一种嵌入式系统启动方法及装置、计算机存储介质

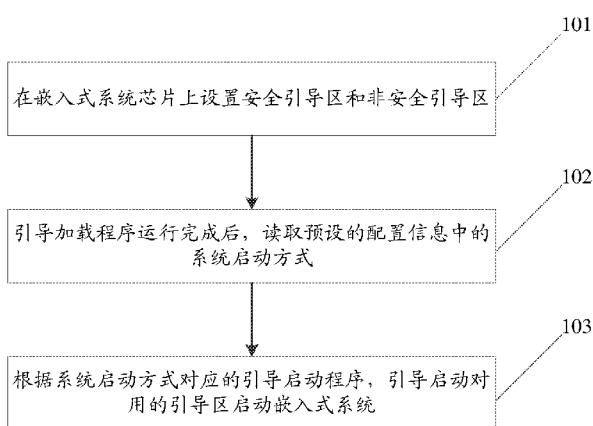


图 1

- 101 SET A SAFETY BOOT AREA AND A NON-SAFETY
BOOT AREA ON A CHIP OF AN EMBEDDED SYSTEM
- 102 AFTER A BOOT LOADER COMPLETES RUNNING,
READ A SYSTEM STARTUP MODE IN PRESET
CONFIGURATION INFORMATION
- 103 BOOT AND START, ACCORDING TO THE BOOT
INITIATOR CORRESPONDING TO THE SYSTEM
STARTUP MODE, THE CORRESPONDING BOOT
AREA TO START THE EMBEDDED SYSTEM

(57) **Abstract:** Disclosed is a method for starting an embedded system, comprising: setting a safety boot area and a non-safety boot area on a chip of the embedded system, the safety boot area and the non-safety boot area respectively corresponding to different boot initiators; after a boot loader completes running, reading preset configuration information, which at least comprises a system startup mode; and executing a boot initiator corresponding to the system startup mode according to the system startup mode, and booting and starting the corresponding boot area to start the embedded system. Also disclosed are a device for starting an embedded system, and a computer storage medium.

(57) **摘要:** 本发明公开了一种嵌入式系统启动方法, 包括: 在嵌入式系统芯片上设置安全引导区和非安全引导区, 所述安全引导区和非安全引导区各自对应不同的引导启动程序; 引导加载程序运行完成后, 读取预设的配置信息, 所述配置信息至少包括系统启动方式; 根据所述系统启动方式执行所述系统启动方式对应的引导启动程序, 引导启动对应的引导区启动嵌入式系统。本发明还同时公开了一种嵌入式系统启动装置、计算机存储介质。

WO 2018/176707 A1

一种嵌入式系统启动方法及装置、计算机存储介质

相关申请的交叉引用

本申请基于申请号为 201710208114.9、申请日为 2017 年 03 月 31 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的
5 全部内容在此引入本申请作为参考。

技术领域

本发明涉及嵌入式系统技术领域，尤其涉及一种嵌入式系统启动方法及装置、计算机存储介质。

背景技术

10 随着科学技术的不断发展，嵌入式设备被广泛应用于人们的日常生活中。其中，嵌入式系统（Embedded System）是嵌入式设备的核心组成部分；所谓嵌入式系统，是一种完全嵌入受控器件内部，为特定应用而定制设计的专用计算机系统，嵌入式系统可用于控制、监视或辅助各种设备、机器或用于工厂运作的设备。嵌入式系统与个人计算机这样的通用计算机系统
15 不同，嵌入式系统通常执行的是带有特定要求的预先定义的任务。由于嵌入式系统只针对一项特殊的任务，相关设计人员可以对嵌入式系统进行优化，减小尺寸、降低成本。嵌入式系统通常会进行大量生产，所以单个的成本节约，可以能够随着产量的提升进行成倍的放大。

目前，嵌入式系统的引导程序仅支持启动一种模式的嵌入式系统，如：
20 引导启动安全模式的嵌入式系统，或引导启动非安全模式的嵌入式系统。如果需要从启动一种模式的嵌入式系统切换至启动另一种模式的嵌入式系统，就需要相关人员重新编写启动代码并重新投片生产，将重新编写的启

动代码写入嵌入式系统的相关芯片中，这样，显然会大大增加嵌入式系统的研发周期，耗费大量时间以及人力物力。

发明内容

有鉴于此，本发明实施例期望提供一种嵌入式系统启动方法及装置、
5 计算机存储介质，能由引导程序启动不同模式的嵌入式系统，更灵活方便的引导启动嵌入式系统。

为达到上述目的，本发明实施例提供了一种嵌入式系统启动方法，所述方法包括：

在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导
10 区和非安全引导区各自对应不同的引导启动程序；所述方法还包括：

引导加载程序运行完成后，读取预设的配置信息，所述配置信息至少包括系统启动方式；

根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。

15 上述方法中，所述配置信息设置于一次性可编程 OTP 模块中。

上述方法中，所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统之前，所述方法还包括：

获取第一信息和第二信息，所述第一信息包括第一数字证书和第二验证数字证书；所述第二信息包括第二数字证书和操作系统程序。
20

上述方法中，所述配置信息还包括第一验证数字证书；

所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统，包括：

当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导
25 启动程序时，所述引导启动程序以所述第一验证数字证书为准，对所述第

一信息中的第一数字证书进行第一次验证;

所述第一次验证通过后,以第一信息中的第二验证数字证书为准,对第二信息中的第二数字证书进行第二次验证;

所述第二次验证通过后,判断所述第二信息中的操作系统程序是否加密,确定操作系统程序被加密、且所述配置信息中还包括解密密钥时,使用所述解密密钥对所述操作系统程序进行解密;

所述操作系统程序解密成功后,启动安全引导区。

上述方法中,所述第一次验证包括:以所述配置信息中的第一验证数字证书为准,验证所述第一信息中的第一数字证书是否与所述第一验证数字证书相同,相同时,所述第一次验证通过;

所述第二次验证包括:以第一信息中的第二验证数字证书为准,验证所述第二信息中的第二数字证书是否与所述第二验证数字证书相同,相同时,所述第二次验证通过。

上述方法中,所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序,引导启动对应的引导区启动嵌入式系统,包括:

当所述系统启动方式对应的引导启动程序为对应于非安全引导区的引导程序时,所述引导程序直接启动非安全引导区。

本发明实施例还提供了一种嵌入式系统启动装置,所述装置包括:设置模块、读取模块、引导模块;其中,

设置模块,配置为在嵌入式系统芯片上设置安全引导区和非安全引导区,所述安全引导区和非安全引导区各自对应不同的引导启动程序;

读取模块,配置为在引导加载程序运行完成后,读取预设的配置信息,所述配置信息至少包括系统启动方式;

引导启动模块,配置为根据所述系统启动方式执行所述系统启动方式对应的引导启动程序,引导启动对应的引导区启动嵌入式系统。

上述装置中，所述装置还包括：OTP 模块，配置为存储所述配置信息。

上述装置中，所述读取模块还配置为：获取第一信息和第二信息，所述第一信息包括第一数字证书和第二验证数字证书；所述第二信息包括第二数字证书和操作系统程序。

5 上述装置中，所述读取模块读取的配置信息还包括第一验证数字证书；
所述引导启动模块还配置为：

当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导启动程序时，所述引导启动程序以所述第一验证数字证书为准，对所述第一信息中的第一数字证书进行第一次验证；

10 所述第一次验证通过后，以第一信息中的第二验证数字证书为准，对第二信息中的第二数字证书进行第二次验证；

所述第二次验证通过后，判断所述第二信息中的操作系统程序是否加密，确定操作系统程序被加密、且所述配置信息中还包括解密密钥时，使用所述解密密钥对所述操作系统程序进行解密；

15 所述操作系统程序解密成功后，启动安全引导区。

上述装置中，所述引导启动模块还配置为：在第一次验证中，以所述配置信息中的第一验证数字证书为准，验证所述第一信息中的第一数字证书是否与所述第一验证数字证书相同，相同时，所述第一次验证通过；

在第二次验证中，以第一信息中的第二验证数字证书为准，验证所述
20 第二信息中的第二数字证书是否与所述第二验证数字证书相同，相同时，
所述第二次验证通过。

上述装置中，所述引导启动模块还配置为：当所述系统启动方式对应的引导启动程序为对应于非安全引导区的引导程序时，所述引导程序直接启动非安全引导区。

25 本发明实施例还提供一种计算机存储介质，该计算机存储介质存储有

计算机程序，该计算机程序配置为执行上述嵌入式系统启动方法。

本发明实施例提供的嵌入式系统启动方法及装置、计算机存储介质，在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导区和非安全引导区各自对应不同的引导启动程序；引导加载程序运行完成后，
5 读取预设的配置信息，所述配置信息至少包括系统启动方式；根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。如此，可以通过引导启动程序引导启动安全引导区启动嵌入式系统、或引导启动非安全引导区启动嵌入式系统，使得嵌入式系统的应用更加广泛，更灵活方便的引导启动嵌入式系统；并且，由于
10 不需要重新编写启动代码并重新投片生产，可以大大缩短嵌入式系统的研发周期，避免时间以及人力物力的耗费。

附图说明

- 图 1 为本发明实施例嵌入式系统启动方法的流程示意图；
图 2 为本发明实施例确定嵌入式系统启动方式的流程示意图；
15 图 3 为本发明实施例嵌入式系统启动方法的总流程示意图；
图 4 为本发明实施例确定嵌入式系统安全状态的流程示意图；
图 5 为本发明实施例启动嵌入式安全系统流程示意图；
图 6 为本发明实施例启动嵌入式安全系统详细示意图；
图 7 为本发明实施例启动嵌入式非安全系统示意图；
20 图 8 为本发明实施例嵌入式系统启动装置的组成结构示意图。

具体实施方式

下面结合附图及具体实施例对本发明再作进一步详细说明。

图 1 为本发明实施例嵌入式系统启动方法的流程示意图，如图 1 所示，本发明实施例嵌入式系统启动方法包括：

步骤 101: 在嵌入式系统芯片上设置安全引导区和非安全引导区, 所述安全引导区和非安全引导区各自对应不同的引导启动程序;

步骤 102: 引导加载程序运行完成后, 读取预设的配置信息, 所述配置信息至少包括系统启动方式;

5 其中, 所述配置信息, 所述配置信息设置于一次性可编程 (OTP, One Time Programmable) 模块中。

步骤 103: 根据所述系统启动方式执行所述系统启动方式对应的引导启动程序, 引导启动对应的引导区启动嵌入式系统。

上述步骤 103 之前, 本发明实施例嵌入式系统的启动方法还包括: 获取第一信息和第二信息, 所述第一信息包括第一数字证书和第二验证数字证书; 所述第二信息包括第二数字证书和操作系统程序;

其中, 当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导启动程序、且所述配置信息还包含第一验证数字证书时, 所述引导启动程序以所述第一验证数字证书为准, 对所述第一信息中的第一数字证书进行第一次验证;

所述第一次验证通过后, 以第一信息中的第二验证数字证书为准, 对第二信息中的第二数字证书进行第二次验证;

所述第二次验证通过后, 判断所述第二信息中的操作系统程序是否加密, 确定操作系统程序被加密、且配置信息中还包含解密密钥时, 使用所述解密密钥对所述操作系统程序进行解密;

所述操作系统程序解密成功后, 启动安全引导区。

当所述系统启动方式为对应于非安全引导区的引导程序时, 所述引导程序直接启动非安全引导区。

下面以具体实施例对本发明嵌入式启动方法进行详细描述说明:

25 图 2 为本发明实施例确定嵌入式系统启动方式的流程示意图, 本发明

实施例中所述配置信息是预先设置的安全状态字段，如图 2 所示，本发明实施例确定嵌入式系统启动方式包括：

步骤 201：读取嵌入式系统中 OTP 中预先设置的安全状态字段；

在实际应用中，OTP 中预先设置的安全状态字段可以根据嵌入式系统
5 实际应用场景进行设定，所述安全状态字段录入 OTP 后即不可再次更改；

步骤 202：确定嵌入式系统启动方式；

步骤 203：如果确定为安全启动方式，则对嵌入式系统镜像文件进行验证签名和解密；

所述步骤 203 之前还包括：根据所述嵌入式系统芯片中的空片标志，
10 确定出嵌入式系统芯片是否为空片，如果是空片，则停止启动嵌入式系统；

如果不是空片，则读取所述 OTP 中的 mk_en 字段，根据所述 mk_en 字段判断是否存在 MKID 信息，如果所述 mk_en 为 1，则确定存在 MKID 信息，判断所述 MKID 信息与第一级嵌入式系统镜像中的 MKID 信息是否一致，如果所述 MKID 不一致，则停止启动嵌入式系统；其中，所述 mk_en
15 字段表示 OTP 中是否存储有嵌入式芯片身份识别信息，所述 MKID 为嵌入式芯片身份识别信息；

如果所述 MKID 一致，则进一步判断 OTP 中的第一验证数字证书 BL_KEY0 是否与第一级嵌入式系统镜像中数字证书中的 RSA 密钥是否一致，如果 BL_KEY0 与 RSA 密钥不一致，则停止启动嵌入式系统；

20 如果 BL_KEY 与 RSA 密钥一致，则对第一级嵌入式系统镜像进行验证签名，如果验证签名不成功，则停止启动嵌入式系统；

如果验证签名成功，则判断第二验证数字证书 BL_KEY1 与第二级镜像中数字证书中的 RSA 密钥是否一致，如果 BL_KEY1 与第二级镜像中数字证书中的 RSA 密钥不一致，则停止启动嵌入式系统；

25 如果 BL_KEY1 与第二级镜像中数字证书中的 RSA 密钥一致，则对第

二级镜像进行解密，如果对第二级镜像解密不成功，则停止启动嵌入式系统；

如果对第二级镜像解密成功，则引导启动安全引导区启动嵌入式系统；

步骤 204：启动嵌入式系统，之后结束本次处理流程；

5 其中，运行通过验证签名和解密后的嵌入式系统镜像，启动安全嵌入式系统。

步骤 205：如果确定为非安全启动方式，则以非安全模式启动嵌入式系统；

其中，如果确定嵌入式系统启动方式为非安全方式，表明嵌入式系统
10 镜像不需要进行验证签名和解密即可运行，根据 Flash 存储器中的空片标志，确定出嵌入式系统装置是否为空片，如果是空片，则停启动安全嵌入式系统；

如果不是空片，将所述 Flash 存储器中的系统镜像存入嵌入式系统的 RAM 存储器中，启动嵌入式系统。

15 上述步骤 201 之前，本发明实施例的方法还可以包括：执行固化程序及初始化的步骤，具体如图 3 所示。

图 3 为本发明实施例嵌入式系统启动方法的总流程示意图，如图 3 所示，本发明实施例嵌入式系统启动方法的处理流程包括：

步骤 301：嵌入式系统上电后，执行固化在 ROM 存储器中的程序；

20 在实际应用中，所述固化在 ROM 存储器中的程序是 BootLoader 程序，所述 BootLoader 程序用于初始化嵌入式硬件设备、建立内存空间映射图，将嵌入式系统中软硬件环境调整至工作状态，为调用操作嵌入式系统内核准备好运行环境；所述 Boot Loader 程序根据嵌入式系统装置体系的不用而不同，同时 Boot Loader 程序也依赖于嵌入式硬件设备的配置，因此，Boot
25 Loader 程序并不通用，对于不同的嵌入式设备而言，即使不同的嵌入式设

备使用一致的装置体系进行构建，如果正常运行在一种嵌入式设备上的 Boot Loader 程序需要在另一种嵌入式设备上正常运行，也通常需要对 Boot Loader 程序进行针对性修改。

步骤 302：初始化配置，将 Flash 存储器中嵌入式系统镜像文件存入
5 RAM 存储器中；

步骤 303：读取嵌入式系统中 OTP 中预先设置的安全状态字段；

在实际应用中，OTP 中预先设置的安全状态字段可以根据嵌入式系统实际应用场景进行设定，所述安全状态字段录入 OTP 后即不可再次更改；

步骤 304：确定嵌入式系统启动方式，如果确定为安全启动方式，则执
10 行步骤 305，如果确定为非安全启动方式，则执行步骤 307；

步骤 305：对嵌入式系统镜像文件进行验证签名和解密；

步骤 306：启动嵌入式系统，之后结束本次处理流程；

步骤 307：以非安全模式启动嵌入式系统。

图 4 为本发明实施例确定嵌入式系统安全状态的流程示意图，如图 4
15 所示，在实际应用中，确定嵌入式安全状态流程具体包括以下步骤：

步骤 401：读取 OTP 中启动方式字段；

步骤 402：当所述启动方式字段代码为 1 时，表示需要安全引导启动嵌入式系统，执行步骤 404；如所述启动方式字段代码为 0 时，表示需要非安全引导启动嵌入式系统，执行步骤 403；

20 步骤 403：启动嵌入式系统，之后结束本次处理流程；

其中，将嵌入式系统镜像加载入嵌入式系统 RAM 存储器后，以非安全引导程序引导启动嵌入式系统，无需对嵌入式系统镜像进行验证签名和解密；

步骤 404：对嵌入式系统镜像验证签名和解密；

25 在实际应用中，当以安全引导方式启动嵌入式系统时，表明需要对嵌

入式系统镜像进行验证签名和解密，只有当验证签名成功和解密成功同时完成后，再运行加载入 RAM 存储器中的嵌入式系统镜像，完成启动嵌入式系统；如果所述验证签名和解密任意一个没有通过验证或解密失败，则停止启动当前嵌入式系统。

5 图 5 为本发明实施例启动嵌入式安全系统流程示意图，如图 5 所示，在实际应用中，启动安全嵌入式系统流程具体包括以下步骤：

步骤 501：读取嵌入式系统芯片中的空片标志；

所述空片标志表征嵌入式系统装置是否已烧录入操作系统程序；

步骤 502：判断嵌入式系统装置是否为空片，如果是空片，执行步骤
10 513；如果不是空片，执行步骤 503；

步骤 503：读取 OTP 中的 mk_en 字段，其中，mk_en 字段表示是否存储有嵌入式芯片身份标识信息；

步骤 504：判断 mk_en 字段是否等于 1，如果等于 1，确定存在 MKID，
15 执行步骤 505；如果不等于 1，确定不存在 MKID，跳过步骤 505，执行步骤 506；

步骤 505：判断 OTP 中 MKID 是否与第一镜像中的 MKID 一致，如果一致，执行步骤 506；如果不一致，执行步骤 513；

其中，所述 MKID 为嵌入式系统芯片表示信息；

步骤 506：判断 OTP 中 BL_KEY0 是否与第一级嵌入式系统镜像数字
20 证书中的 RSA 密钥一致，如果一致，执行步骤 507；如果不一致，执行步骤 513；

步骤 507：对第一级嵌入式系统镜像进行验证签名；

步骤 508：判断验证签名是否成功，如果成功，执行步骤 509；如果不成功，执行步骤 513；

25 步骤 509：判断 BK_KEY1 是否与第二镜像数字证书中 RSA 密钥一致，

如果一致，执行步骤 510；如果不一致，执行步骤 513；

步骤 510：对第二级嵌入式系统镜像进行解密；

步骤 511：判断第二镜像解密是否成功，如果成功，执行步骤 512；如果不成功，执行步骤 513；

5 步骤 512：启动嵌入式系统，之后结束本次处理流程；

步骤 513：停止启动嵌入式系统。

图 6 为本发明实施例启动嵌入式安全系统详细示意图，如图 6 所示，在实际应用中，嵌入式系统镜像进行验证签名和解密具体包括以下步骤：

步骤 601：使用上一级代码中的第一数字证书或密钥 KEY 信息对嵌入式系统镜像的证书进行验证；对所述第一数字证书或密钥 KEY 信息进行 hash 运算，将获得的固定长度的二进制数值存入第一结果 sign_hash1 中；

其中，如果是对第一级嵌入式系统镜像进行验证签名，则使用 OTP 中预设的 KEY 信息或第一数字证书对所述第一级嵌入式系统镜像证书进行验证签名；如对第二级嵌入式系统镜像进行验证签名，则使用第一级嵌入式系统镜像中的 KEY 信息或第一数字证书对第二级嵌入式系统镜像证书进行验证签名，以此类推；

步骤 602：对步骤 601 中所述嵌入式系统镜像证书或 KEY 信息进行 hash 运算，将获得的固定长度的二进制数值存入第二结果 sign_hash2 中；

步骤 603：判断 sign_hash1 和 sign_hash2 是否相等，如果相等，执行步骤 604；如果不相等，执行步骤 610；

步骤 604：对嵌入式系统镜像代码进行 hash 运算，将获得的固定长度的二进制数值存入系统镜像代码结果 code_hash1 中；

步骤 605：判断嵌入式系统镜像证书中预存的系统镜像代码验证信息 code_hash 与 code_hash1 是否相等，如果相等，执行步骤 607；如果不相等，执行步骤 610；

步骤 606: 判断嵌入式系统镜像是否加密, 如果加密, 执行步骤 607;
如果未加密, 执行步骤 609;

步骤 607: 用 OTP 中的密钥对嵌入式系统镜像进行解密;

步骤 608: 判断解密是否成功, 如果成功, 执行步骤 609; 如果不成功,

5 执行步骤 610;

步骤 609: 运行解密后的嵌入式系统镜像, 启动嵌入式系统, 之后结束
本次处理流程;

步骤 610: 停止启动嵌入式系统。

图 7 为本发明实施例启动嵌入式非安全系统示意图, 如图 7 所示, 确
10 定嵌入式系统为非安全状态, 启动非安全嵌入式系统包括以下步骤:

步骤 701: 读取嵌入式系统芯片空片标志;

步骤 702: 判断嵌入式系统装置是否是空片, 如果是空片, 执行步骤
703; 如果不是空片, 执行步骤 704;

步骤 703: 停止启动嵌入式系统, 之后结束本次处理流程;

15 步骤 704: 运行 RAM 存储器中嵌入式系统镜像, 启动嵌入式系统。

图 8 为本发明实施例嵌入式系统启动装置的结构示意图, 如图 8 所示,
本发明实施例嵌入式系统启动装置包括:

设置模块 801, 配置为在嵌入式系统芯片上设置安全引导区和非安全引
导区, 所述安全引导区和非安全引导区各自对应不同的引导启动程序;

20 读取模块 802, 配置为在引导加载程序运行完成后, 读取预设的配置信
息, 所述配置信息至少包括系统启动方式;

引导启动模块 803, 配置为根据所述系统启动方式执行所述系统启动方
式对应的引导启动程序, 引导启动对应的引导区启动嵌入式系统;

其中, 所述装置还包括: OTP 模块 804, 配置为存储所述配置信息;

25 所述读取模块 802, 还配置为: 获取第一信息和第二信息, 所述第一信

息包括第一数字证书和第二验证数字证书；所述第二信息包括第二数字证书和操作系统程序；

所述引导启动模块 803 还配置为：

当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导启动程序时，所述引导启动程序以所述第一验证数字证书为准，对所述第一信息中的第一数字证书进行第一次验证；

所述第一次验证通过后，以第一信息中的第二验证数字证书为准，对第二信息中的第二数字证书进行第二次验证；

所述第二次验证通过后，判断所述第二信息中的操作系统程序是否加密，确定操作系统程序被加密、且所述配置信息中还包括解密密钥时，使用所述解密密钥对所述操作系统程序进行解密；

所述操作系统程序解密成功后，启动安全引导区；

其中，所述第一次验证包括：以所述配置信息中的第一验证数字证书为准，验证所述第一信息中的第一数字证书是否与所述第一验证数字证书相同，相同时，所述第一次验证通过；

所述第二次验证包括：以第一信息中的第二验证数字证书为准，验证所述第二信息中的第二数字证书是否与所述第二验证数字证书相同，相同时，所述第二次验证通过；

所述引导启动模块 803 还配置为：当所述系统启动方式对应的引导启动程序为对应于非安全引导区的引导程序时，所述引导程序直接启动非安全引导区。

在实际应用中，所述设置模块 801、读取模块 802、引导启动模块 803 均可由嵌入式系统中的中央处理器（CPU，Central Processing Unit）、微处理器（MPU，Micro Processor Unit）、数字信号处理器（DSP，Digital Signal Processor）、或现场可编程门阵列（FPGA，Field Programmable Gate Array）

等实现。

如上所述，本发明实施例提供的嵌入式系统启动方法及装置，在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导区和非安全引导区各自对应不同的引导启动程序；引导加载程序运行完成后，读取预设的配置信息，所述配置信息至少包括系统启动方式；根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。如此，本发明实施例提供的嵌入式启动方法及装置可以同时兼容启动安全嵌入式系统和非安全嵌入式系统，当用户需要启动另一种嵌入式系统时，不必修改启动嵌入式的引导程序或重新开发新的装置，降低研发周期，节省人力物力。

本发明实施例上述业务信令跟踪的装置如果以软件功能模块的形式实现并作为独立的产品销售或使用，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机、服务器、或者网络设备等）执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read Only Memory）、磁碟或者光盘等各种可以存储程序代码的介质。这样，本发明实施例不限制于任何特定的硬件和软件结合。

相应地，本发明实施例还提供一种计算机存储介质，其中存储有计算机程序，该计算机程序配置为执行本发明实施例的嵌入式系统启动方法。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

工业实用性

本发明实施例的技术方案，在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导区和非安全引导区各自对应不同的引导启动程序；引导加载程序运行完成后，读取预设的配置信息，所述配置信息至少
5 包括系统启动方式；根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。如此，可以通过引导启动程序引导启动安全引导区启动嵌入式系统、或引导启动非安全引导区启动嵌入式系统，使得嵌入式系统的应用更加广泛，更灵活方便的引导启动嵌入式系统；并且，由于不需要重新编写启动代码并重新投片生产，
10 可以大大缩短嵌入式系统的研发周期，避免时间以及人力物力的耗费。

权利要求书

1、一种嵌入式系统启动方法，在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导区和非安全引导区各自对应不同的引导启动程序；所述方法还包括：

5 引导加载程序运行完成后，读取预设的配置信息，所述配置信息至少包括系统启动方式；

根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。

2、根据权利要求1所述的方法，其中，所述配置信息设置于一次性
10 可编程 OTP 模块中。

3、根据权利要求1或2所述的方法，其中，所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统之前，所述方法还包括：

获取第一信息和第二信息，所述第一信息包括第一数字证书和第二
15 验证数字证书；所述第二信息包括第二数字证书和操作系统程序。

4、根据权利要求3所述的方法，其中，所述配置信息还包括第一验证数字证书；

所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统，包括：

20 当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导启动程序时，所述引导启动程序以所述第一验证数字证书为准，对所述第一信息中的第一数字证书进行第一次验证；

所述第一次验证通过后，以第一信息中的第二验证数字证书为准，对第二信息中的第二数字证书进行第二次验证；

25 所述第二次验证通过后，判断所述第二信息中的操作系统程序是否

加密，确定操作系统程序被加密、且所述配置信息中还包括解密密钥时，使用所述解密密钥对所述操作系统程序进行解密；

所述操作系统程序解密成功后，启动安全引导区。

5 5、根据权利要求4所述的方法，其中，所述第一次验证包括：以所述配置信息中的第一验证数字证书为准，验证所述第一信息中的第一数字证书是否与所述第一验证数字证书相同，相同时，所述第一次验证通过；

所述第二次验证包括：以第一信息中的第二验证数字证书为准，验证所述第二信息中的第二数字证书是否与所述第二验证数字证书相同，
10 相同时，所述第二次验证通过。

6、根据权利要求1所述的方法，其中，所述根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统，包括：

当所述系统启动方式对应的引导启动程序为对应于非安全引导区的
15 引导程序时，所述引导程序直接启动非安全引导区。

7、一种嵌入式系统启动装置，所述装置包括：设置模块、读取模块、引导模块；其中，

设置模块，配置为在嵌入式系统芯片上设置安全引导区和非安全引导区，所述安全引导区和非安全引导区各自对应不同的引导启动程序；

20 读取模块，配置为在引导加载程序运行完成后，读取预设的配置信息，所述配置信息至少包括系统启动方式；

引导启动模块，配置为根据所述系统启动方式执行所述系统启动方式对应的引导启动程序，引导启动对应的引导区启动嵌入式系统。

8、根据权利要求7所述的装置，其中，所述装置还包括：OTP模块，
25 配置为存储所述配置信息。

9、根据权利要求 7 或 8 所述的装置，其中，所述读取模块还配置为：获取第一信息和第二信息，所述第一信息包括第一数字证书和第二验证数字证书；所述第二信息包括第二数字证书和操作系统程序。

10、根据权利要求 9 所述的装置，其中，所述读取模块读取的配置信息还包括第一验证数字证书；

所述引导启动模块还配置为：

当所述系统启动方式对应的引导启动程序为对应于安全引导区的引导启动程序时，所述引导启动程序以所述第一验证数字证书为准，对所述第一信息中的第一数字证书进行第一次验证；

10 所述第一次验证通过后，以第一信息中的第二验证数字证书为准，对第二信息中的第二数字证书进行第二次验证；

所述第二次验证通过后，判断所述第二信息中的操作系统程序是否加密，确定操作系统程序被加密、且所述配置信息中还包括解密密钥时，使用所述解密密钥对所述操作系统程序进行解密；

15 所述操作系统程序解密成功后，启动安全引导区。

11、根据权利要求 10 所述的装置，其中，所述引导启动模块还配置为：在第一次验证中，以所述配置信息中的第一验证数字证书为准，验证所述第一信息中的第一数字证书是否与所述第一验证数字证书相同，相同时，所述第一次验证通过；

20 在第二次验证中，以第一信息中的第二验证数字证书为准，验证所述第二信息中的第二数字证书是否与所述第二验证数字证书相同，相同时，所述第二次验证通过。

12、根据权利要求 7 所述的装置，其中，所述引导启动模块还配置为：当所述系统启动方式对应的引导启动程序为对应于非安全引导区的引导程序时，所述引导程序直接启动非安全引导区。

25

13、一种计算机存储介质，所述计算机存储介质中存储有计算机可执行指令，该计算机可执行指令配置为执行权利要求 1-6 任一项所述的嵌入式系统启动方法。

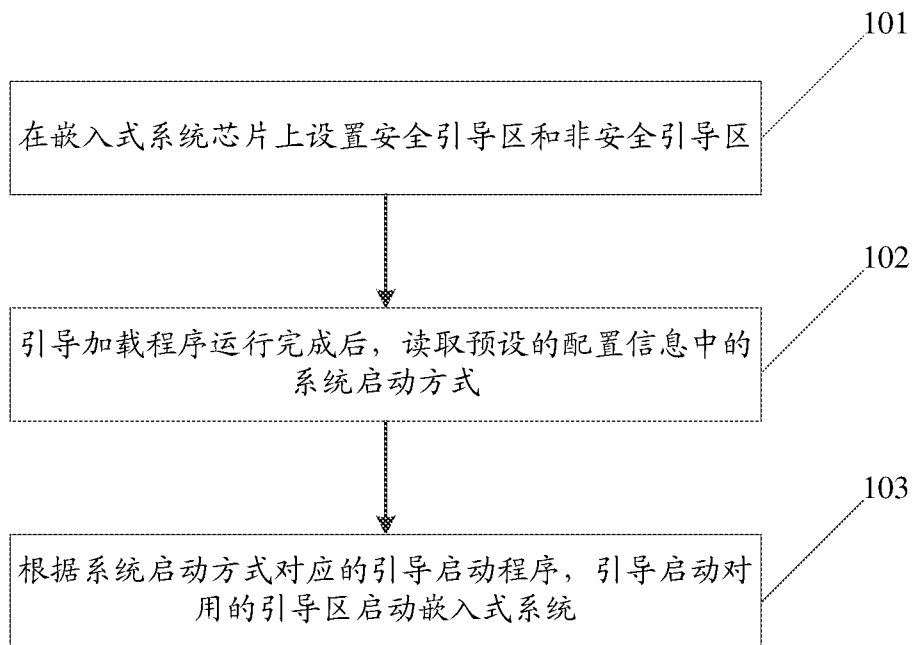


图 1

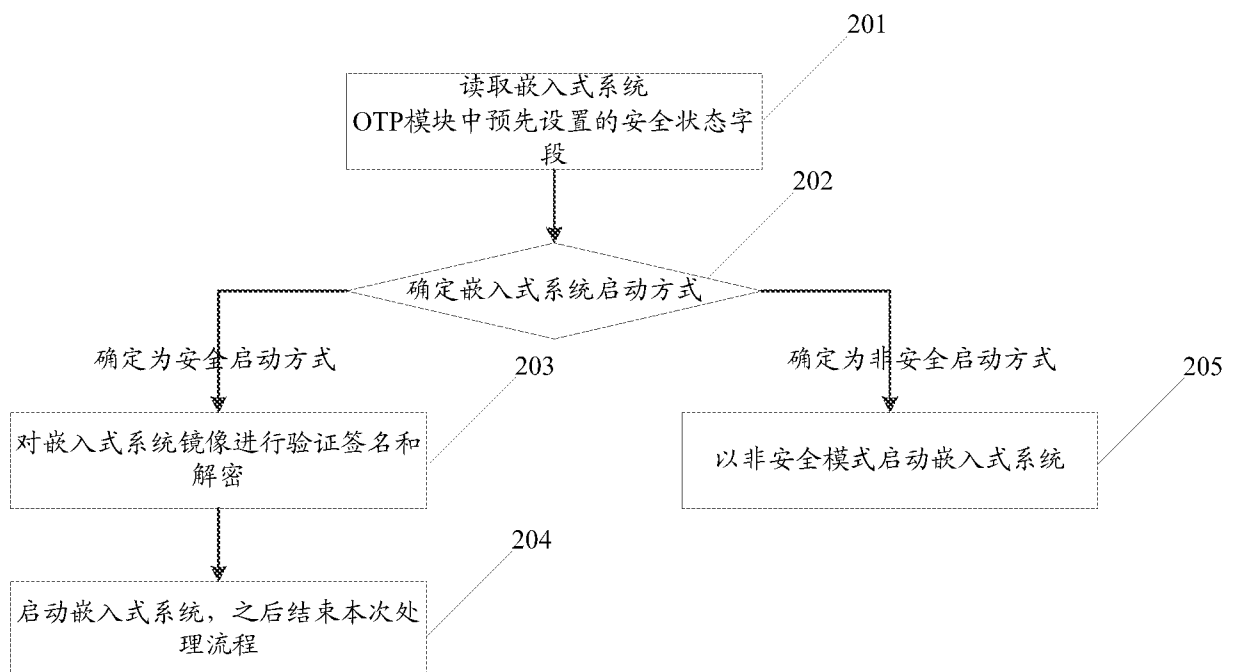


图 2

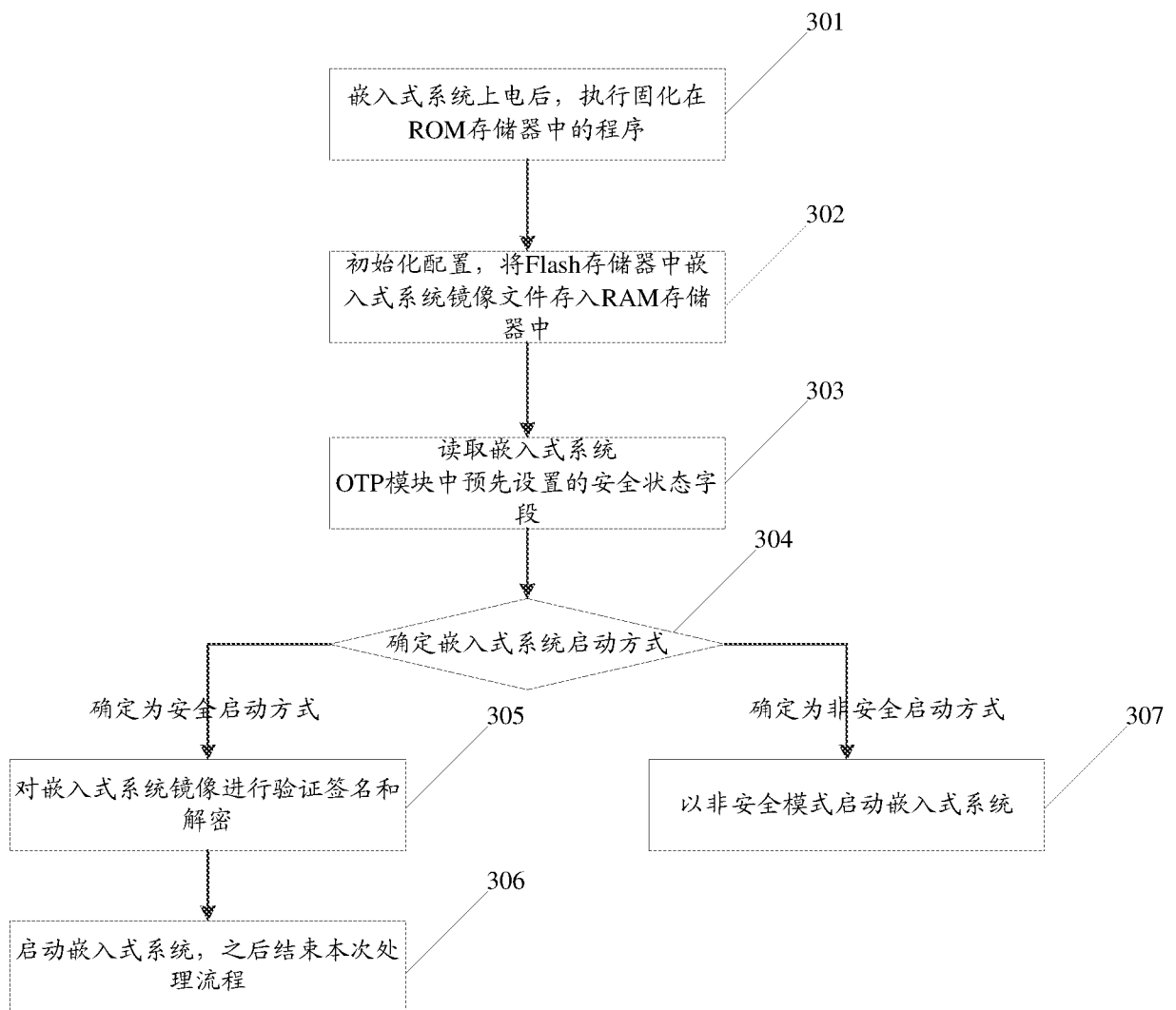


图 3

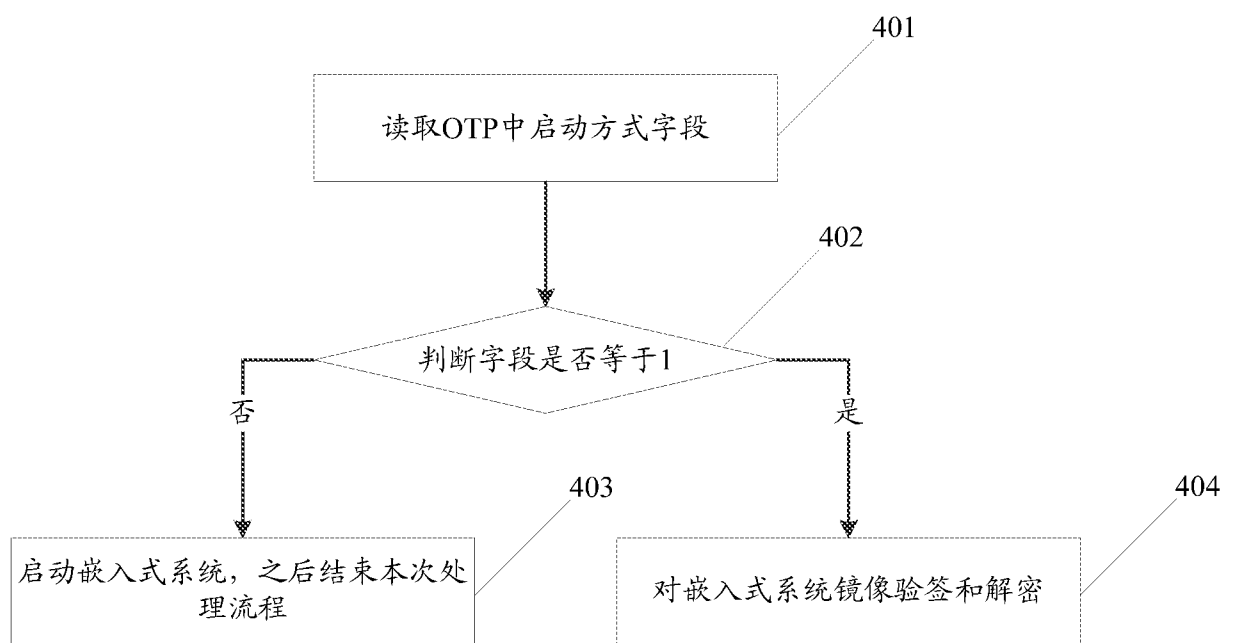


图 4

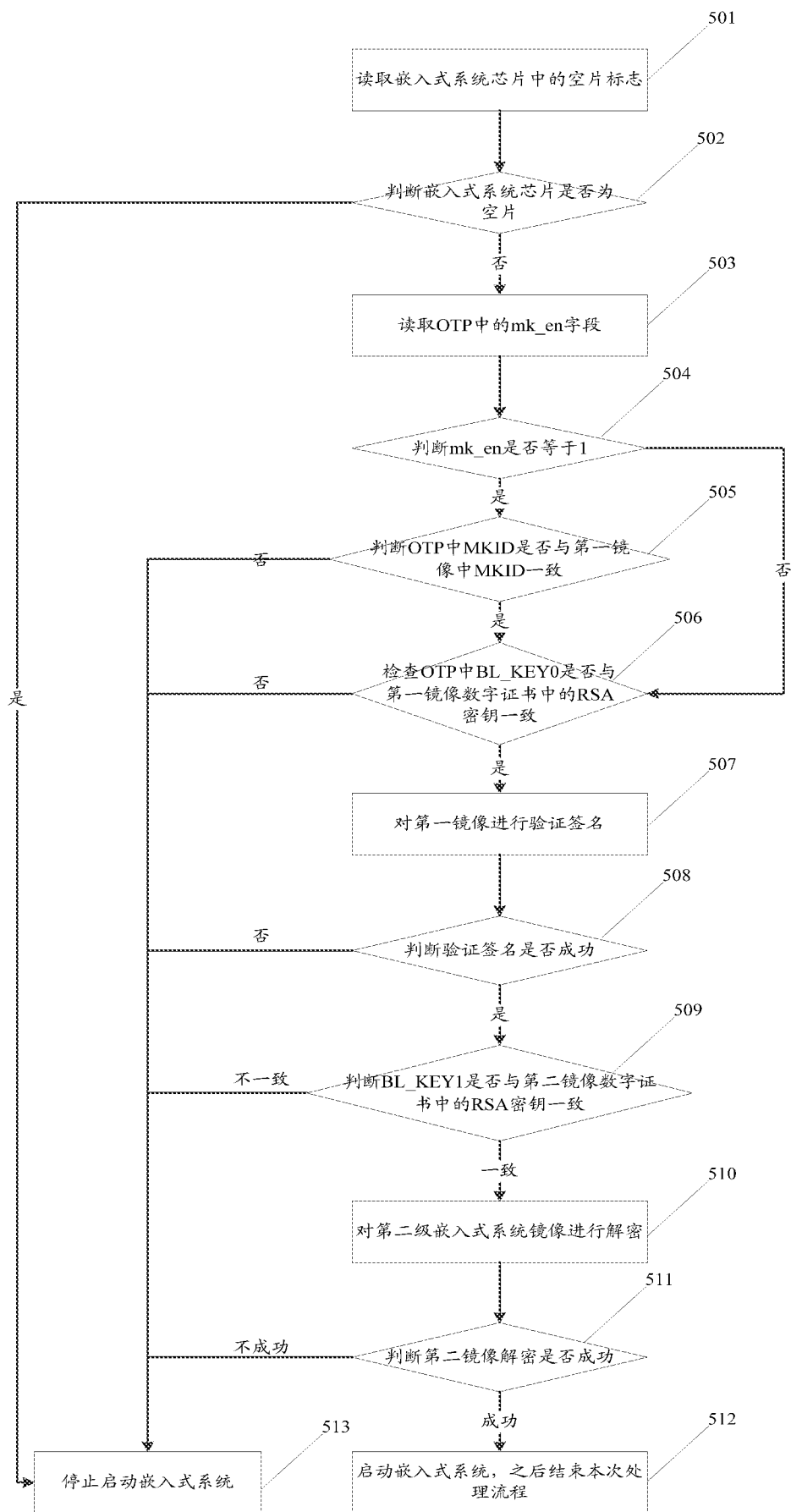


图 5

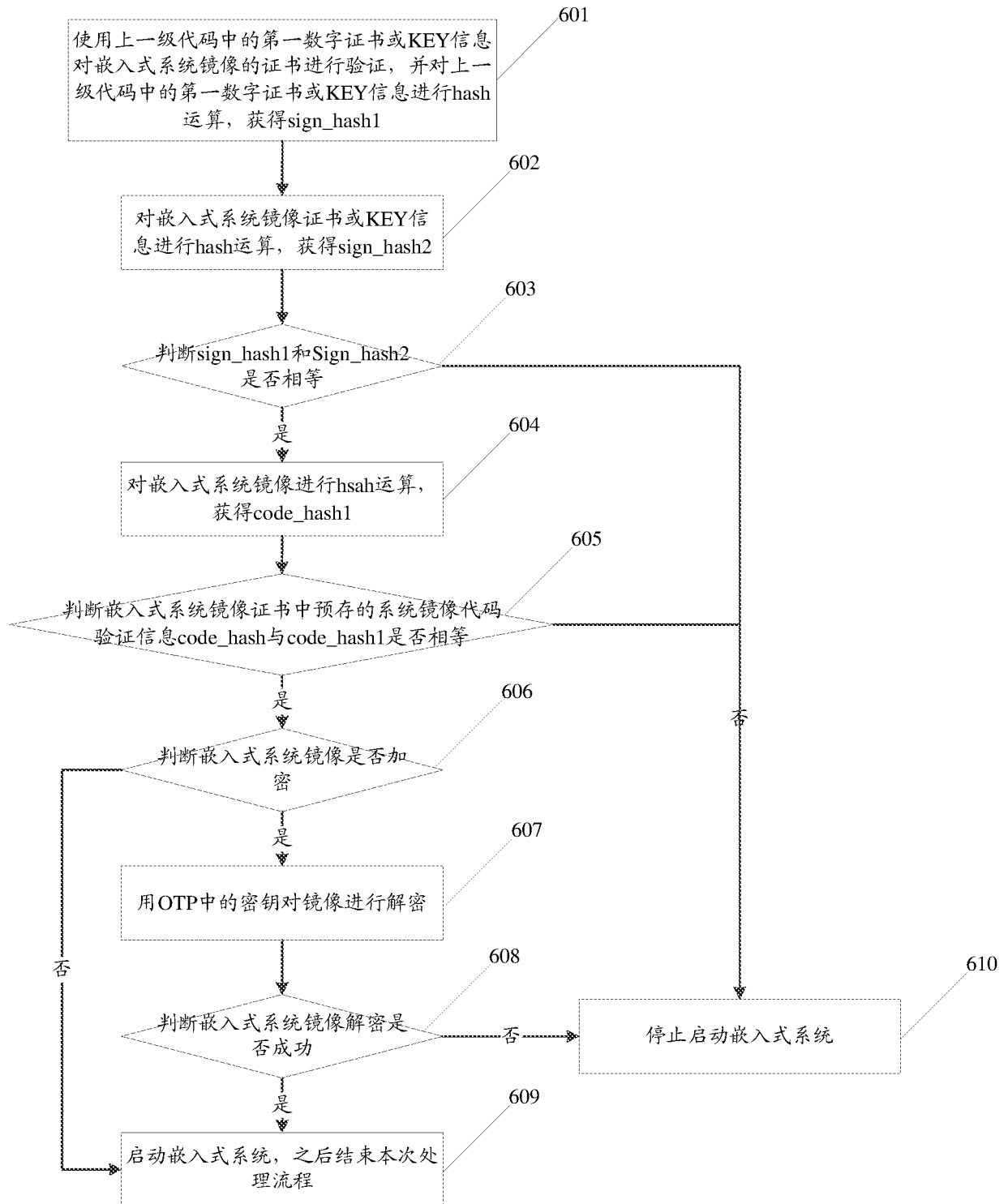


图 6

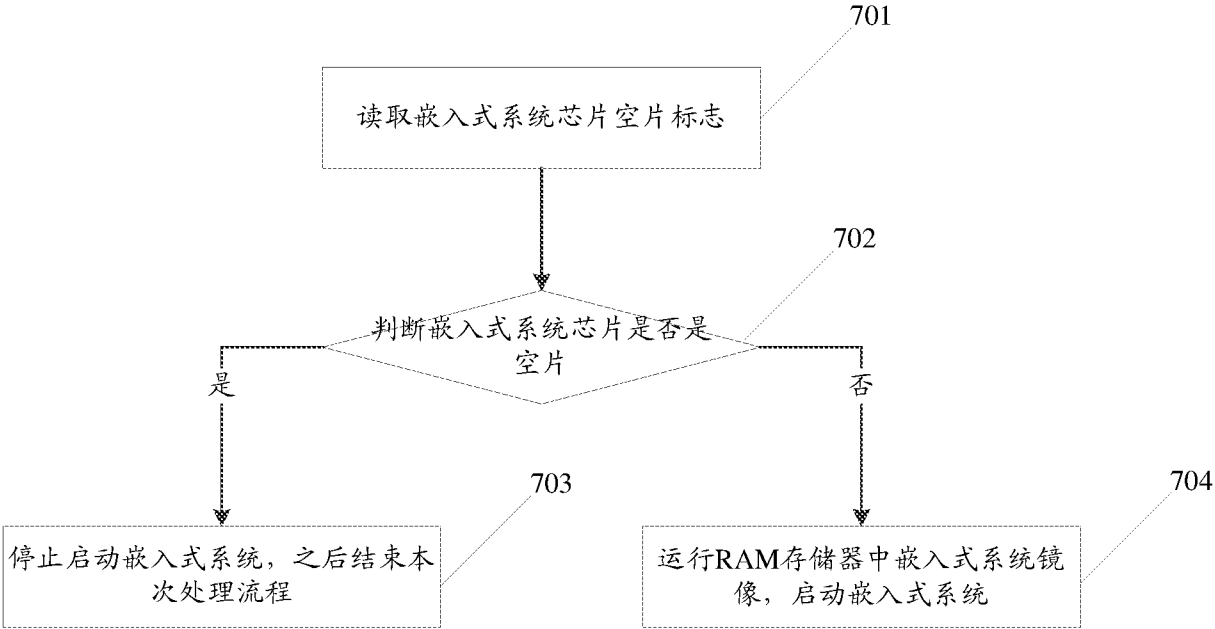


图 7

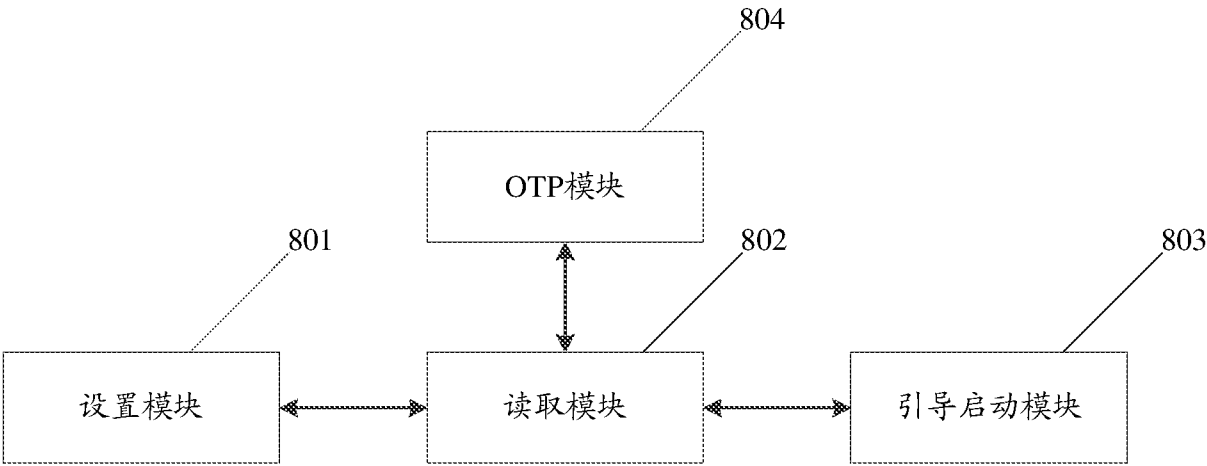


图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/095333

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/445 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNKI, DWPI; 嵌入式, 引导, 启动, 加载, 验证, 证书, 签名, 初始化, 不同, 多个, 区, 块, 区域, 模式, 方式; load, boot, launch, initiate, verify, authenticate, certificate, signature, different, multiple, region, district, partition, division, block, mode, pattern

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101699402 A (CORE TECHNOLOGY SUZHOU CO., LTD.) 28 April 2010 (28.04.2010), description, paragraphs [0004]-[0061], and figures 1 and 2	1-3, 6-9, 12, 13
A	CN 101826027 A (SHENZHEN TEMOBI SCIENCE & TECHNOLOGY DEVELOPMENT CO., LTD.) 08 September 2010 (08.09.2010), entire document	1-13
A	CN 104951328 A (IMF ELECTRONICS SHANGHAI CO., LTD. et al.) 30 September 2015 (30.09.2015), entire document	1-13
A	US 6052778 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 18 April 2000 (18.04.2000), entire document	1-13

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 09 November 2017	Date of mailing of the international search report 29 November 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer MENG, Tiange Telephone No. (86-10) 62411653

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/095333

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101699402 A	28 April 2010	CN 101699402 B	27 June 2012
CN 101826027 A	08 September 2010	None	
CN 104951328 A	30 September 2015	None	
US 6052778 A	18 April 2000	None	

A. 主题的分类 G06F 9/445 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																	
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CNKI, DWPI; 嵌入式, 引导, 启动, 加载, 验证, 证书, 签名, 初始化, 不同, 多个, 区, 块, 区域, 模式, 方式; load, boot, launch, initiate, verify, authenticate, certificate, signature, different, multiple, region, district, partition, division, block, mode, pattern																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101699402 A (苏州国芯科技有限公司) 2010年 4月 28日 (2010 - 04 - 28) 说明书第4-61段、图1-2</td> <td>1-3, 6-9, 12-13</td> </tr> <tr> <td>A</td> <td>CN 101826027 A (深圳市融创天下科技发展有限公司) 2010年 9月 8日 (2010 - 09 - 08) 全文</td> <td>1-13</td> </tr> <tr> <td>A</td> <td>CN 104951328 A (国基电子上海有限公司 等) 2015年 9月 30日 (2015 - 09 - 30) 全文</td> <td>1-13</td> </tr> <tr> <td>A</td> <td>US 6052778 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2000年 4月 18日 (2000 - 04 - 18) 全文</td> <td>1-13</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101699402 A (苏州国芯科技有限公司) 2010年 4月 28日 (2010 - 04 - 28) 说明书第4-61段、图1-2	1-3, 6-9, 12-13	A	CN 101826027 A (深圳市融创天下科技发展有限公司) 2010年 9月 8日 (2010 - 09 - 08) 全文	1-13	A	CN 104951328 A (国基电子上海有限公司 等) 2015年 9月 30日 (2015 - 09 - 30) 全文	1-13	A	US 6052778 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2000年 4月 18日 (2000 - 04 - 18) 全文	1-13
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	CN 101699402 A (苏州国芯科技有限公司) 2010年 4月 28日 (2010 - 04 - 28) 说明书第4-61段、图1-2	1-3, 6-9, 12-13															
A	CN 101826027 A (深圳市融创天下科技发展有限公司) 2010年 9月 8日 (2010 - 09 - 08) 全文	1-13															
A	CN 104951328 A (国基电子上海有限公司 等) 2015年 9月 30日 (2015 - 09 - 30) 全文	1-13															
A	US 6052778 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2000年 4月 18日 (2000 - 04 - 18) 全文	1-13															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																	
国际检索实际完成的日期 2017年 11月 9日		国际检索报告邮寄日期 2017年 11月 29日															
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 孟田革 电话号码 (86-10) 62411653															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/095333

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	101699402	A	2010年 4月 28日	CN 101699402 B	2012年 6月 27日
CN	101826027	A	2010年 9月 8日	无	
CN	104951328	A	2015年 9月 30日	无	
US	6052778	A	2000年 4月 18日	无	