(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
2019 年 4 月 4 日 (04.04.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/062993 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2018/108857

(22) 国际申请日: 2018 年 9 月 29 日 (29.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710928376.2 2017年9月30日 (30.09.2017) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 许世峰 (**XU, Shifeng**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈 溪 (**CHEN, Xi**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (**SCIHEAD IP LAW FIRM**); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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,

(54) **Title:** SECURE STARTUP METHOD AND APPARATUS, AND TERMINAL DEVICE

(54) 发明名称: 安全启动方法、装置及终端设备

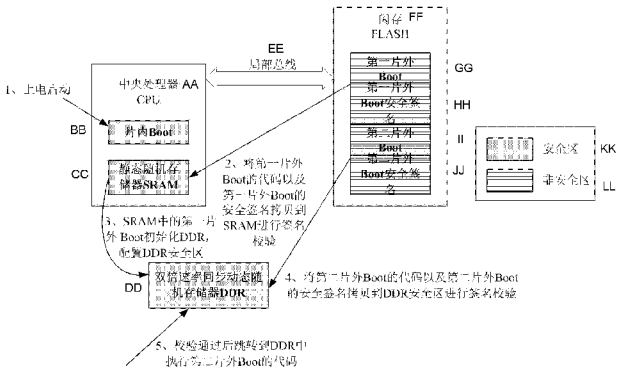

图 2

1 Power-on and startup
2 Copy the code of a first off-chip Boot and a security signature of the first off-chip Boot to an SRAM for signature verification
3 The first off-chip Boot in the SRAM initializes a DDR and configures a secure region of the DDR
4 Copy the code of a second off-chip Boot and a security signature of the second off-chip Boot to the secure region of the DDR for signature verification
5 When the verification is passed, jump to the DDR to execute the code of the second off-chip Boot
AA Central processing unit (CPU)
BB On-chip Boot
CC Static random access memory (SRAM)
DD Double data rate dynamic random memory (DDR)
EE Local bus
FF Flash
GG First off-chip Boot
HH Security signature of first off-chip Boot
II Second off-chip Boot
JJ Security signature of second off-chip Boot
KK Secure region
LL Insecure region

(57) **Abstract:** A secure startup method and apparatus, and terminal device. The method comprises: copying the code and a security signature of a first off-chip Boot to an SRAM for signature verification, wherein the function realized by the first off-chip Boot comprises the initialization of a DDR, and the initialization of the DDR comprises configuring a secure region of the DDR; when the verification of the signature of the first off-chip Boot succeeds, executing the code of the first off-chip Boot in the SRAM, so as to realize the initialization of the DDR and the configuration of the secure region of the DDR; copying the code and a security signature of a second off-chip Boot to the secure region of the DDR for signature verification, wherein the second off-chip Boot is all the other Boots in the off-chip Boot other than the first off-chip Boot; and when the verification of the signature of the second off-chip Boot succeeds, executing the code of the second off-chip Boot in the secure region of the DDR. The embodiments of the present invention can prevent a security flaw in a specific time window in a secure startup process, and improve system security.

WO 2019/062993 A1

[见续页]

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))。

(57) 摘要: 一种安全启动方法、装置及终端设备，该方法包括：将第一片外Boot的代码和安全签名拷贝到SRAM中进行签名校验，第一片外Boot实现的功能包括初始化DDR，初始化DDR包括配置DDR安全区；对第一片外Boot签名校验成功后，在SRAM中执行第一片外Boot的代码，实现初始化DDR以及配置DDR安全区；将第二片外Boot的代码和安全签名拷贝到DDR的安全区进行签名校验，第二片外Boot是片外Boot中除第一片外Boot以外的其他全部Boot；对第二片外Boot签名校验成功后，在DDR的安全区中执行第二片外Boot的代码。本发明实施例能防止安全启动过程中特定时间窗内的安全漏洞，提高系统安全。

安全启动方法、装置及终端设备

本申请要求于2017年09月30日递交中国知识产权局、申请号为2017109283762，发明名称为“安全启动方法、装置及终端设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明实施例涉及计算机领域，尤其涉及一种安全启动方法、装置及终端设备。

背景技术

系统安全是为了支持安全启动以及保证系统在可信环境中运行的一整套软硬件方案。基于ARM架构的系统安全方案通常由安全启动（Secure Boot）和信任区域（Trust Zone）技术结合而成。Secure Boot是系统安全的基础，负责整个安全系统的初始化过程。根据可信的完整性理论，系统的安全启动是整个系统安全的可信根，只有保证了系统启动的安全，才能保证系统其他各部件的安全。

系统安全启动时，系统采取逐级校验签名，校验通过之后引导后续的过程。通常安全签名和代码存储在片外(通常是闪存FLASH)，系统首先由片内Boot启动，对片外启动代码签名校验校验通过后，切换到片外启动代码执行，引导后续启动程序。参见图1，是现有技术中的一种安全启动过程的示意图。如图1所示，片内Boot和静态随机存储器（Static Random Access Memory，SRAM）为安全区。系统上电后首先在片内Boot运行安全启动代码（Boot ROM Secure Boot Code，BSBC），完成必要的初始化配置之后，将下一级节点片外Boot拷贝到SRAM进行签名校验。由于SRAM的成本较高，通常不会超过256KB，远小于片外Boot的大小，拷贝和签名校验动作只能采取多次分段覆盖的方式，无法在安全区保留完整的片外Boot代码，签名校验成功之后，再跳到片外Boot起始地址处启动代码执行。

BSBC对片外Boot的拷贝和签名校验分段进行，拷贝通常走局部总线（localbus）通道速率慢，10M片外Boot的分段拷贝和签名校验时间估计需要2s，签名校验成功之后直接跳转到片外Boot起始地址处启动代码执行。由于片外Boot为非安全区，在这2s的时间窗内通过篡改片外Boot代码能够攻破安全启动流程，因此存在系统安全漏洞。

发明内容

本发明实施例提供了一种安全启动方法、装置及终端设备，能够防止通常安全启动过程中特定时间窗内的安全漏洞，提高了系统安全。

本发明实施例具体可以通过如下技术方案实现:

第一方面，本发明实施例提供了一种安全启动方法，该方法包括：将第一片外Boot的代码以及所述第一片外Boot的安全签名拷贝到静态随机存储器SRAM中进行签名校验，所述第一片外Boot实现的功能包括初始化双倍速率同步动态随机存储器DDR，所述初始化DDR过程包括配置DDR安全区；在对所述第一片外Boot签名校验成功后，在SRAM

中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区；将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区进行签名校验，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot；在对所述第二片外 Boot 签名校验成功后，在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。本发明实施例中，通过增加第一片外 Boot，在 SRAM 中在对第一片外 Boot 签名校验成功后，执行第一片外 Boot 的代码实现初始化 DDR 以及配置所述 DDR 安全区，进而将除第一片外 Boot 以外的其他所有片外 Boot（即本发明实施例中的第二片外 Boot）的签名校验以及执行代码的过程均在 DDR 安全区进行，避免了现有技术中先在 SRAM 安全区进行签名校验之后再跳转到非安全区的 FLASH 中执行代码期间的代码被篡改风险，提高了系统启动过程的安全性。

在一种可能的设计中，所述第一片外 Boot 为片外 Boot 中新增的一级 Boot。本发明实施例中，新增一级 Boot 专门用于初始化 DDR 以及配置 DDR 安全区，从而使得在对第一片外 Boot 签名校验成功后，配置一个容量较大的 DDR 安全区，用于校验第二片外 Boot 以及执行第二片外 Boot 的代码。从而实现第二片外 Boot 的一次性拷贝、校验。解决了签名校验和跳转到片外 Boot 执行的时间窗内（大约 2s）可以篡改片外 Boot（处于非安全区）的安全漏洞。

在一种可能的设计中，所述第一片外 Boot 的容量小于或等于 SRAM 的容量。本发明实施例中，第一片外 Boot 由于功能单一，可以做到小于 128KB（或者 256KB），片内 Boot 能一次性完成第一片外 Boot 的拷贝，从而解决了签名校验和跳转到片外 Boot 执行的时间窗内（大约 2s）可以篡改片外 Boot（处于非安全区）的安全漏洞。

第二方面，本发明实施例提供了一种安全启动装置，该装置包括用于执行上述第一方面所描述的安全启动方法的模块或单元。

第三方面，本发明实施例提供了一种终端设备，该终端设备包括处理器和存储器。其中，所述处理器用于调用所述存储器存储的安全启动程序指令执行上述第一方面所提供的安全启动方法。

第四方面，本发明实施例提供了一种计算机存储介质，用于存储用于执行上述第一方面所述的安全启动方法的计算机软件程序指令，所述程序指令当被所述处理器执行时使所述处理器执行如上述第一方面所述的安全启动方法。

第五方面，本发明实施例提供了一种计算机程序，该程序包括计算机软件程序指令，所述程序指令当被所述处理器执行时使所述处理器执行如上述第一方面所述的安全启动方法。

附图说明

图 1 是现有技术中的一种安全启动过程的示意图；

图 2 是本发明实施例提供的一种安全启动方法的流程示意图；

图 3 是本发明实施例提供的一种签名校验过程的示意图；

图 4 是本发明实施例提供的一种安全启动装置的结构示意图；

图 5 是本发明实施例提供的一种终端设备的结构示意图。

具体实施方式

为了使本发明的技术方案及有益效果更加清楚，以下结合附图及实施例，对本发明进行进一步详细说明。

本发明实施例中的安全启动方法适用于各种带有处理器(Central Processing Unit，简称：CPU)的终端设备，包括服务器、计算设备、车载设备、可穿戴设备、以及各种形式的用户设备(User Equipment，UE)，移动台(Mobile station，MS)，终端(terminal)，终端设备(Terminal Equipment)、嵌入式设备（比如基站设备中的嵌入式单板）等等。其中，CPU 可以是 ARM CPU，或者其他类型 CPU，本发明实施例不作具体限定。

本发明实施例适用于安全启动场景，例如：ARM 架构的系统安全启动。本发明实施例以系统安全启动为例进行说明。

结合图 2，是本发明实施例提供的一种安全启动方法的流程示意图，该方法的执行主体为处理器(CPU)。

步骤 1：系统上电启动。

系统上电后首先在片内启动引导程序（Boot）运行 BSBC，完成必要的初始化配置之后，执行步骤 2。

步骤 2：将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名拷贝到 SRAM 中进行签名校验，签名校验成功后，执行步骤 3，所述第一片外 Boot 实现的功能包括初始化 DDR，所述初始化 DDR 过程包括配置 DDR 安全区。

本发明实施例中，可以将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名一次性拷贝到 SRAM 中。

签名校验的过程具体可以参见图 3。利用第一片外 Boot 的安全签名对第一片外 Boot 的代码进行签名验证，以验证第一片外 Boot 的代码是否被篡改过。

需要说明的是，本发明实施例中的第一片外 Boot 是片外 Boot 新增加的一级 Boot，该新增的片外 Boot 的功能主要完成 DDR 的初始化（设备上的已有硬件），DDR 初始化过程中包括配置 DDR 安全区的过程。初始化 DDR 过程中除配置 DDR 安全区以外的其他过程为现有技术，本发明实施例对此不作特别说明。配置 DDR 安全区可以包括但不限于如下过程：指定某一段地址区间是安全的，只能通过特定的安全的访问方式去访问该段地址区间，而不能采用非安全的访问方式去访问、配置 DDR 安全区的容量。DDR 区域是安全的是因为：DDR 不易被第三方通过软件进行代码篡改，相较于片外存储器（例如 FLASH）来说，安全级别更高。

本发明实施例中，第一片外 Boot 由于功能单一，可以做到小于 128KB（或者 256KB），片内 Boot 能一次性完成第一片外 Boot 的拷贝，从而解决了签名校验和跳转到片外 Boot 执行的时间窗内（大约 2s）可以篡改片外 Boot（处于非安全区）的安全漏洞。

步骤 3：在 SRAM 中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区。

通常的计算机系统，SRAM 容量较小（一般 128KB 或者 256KB），而 DDR 空间容量较大（通常为 1GB 以上）。由于 DDR 空间很大，后续安全启动流程可以将除所述第一片

外 Boot 以外的其他片外 Boot 一次性拷贝到 DDR 安全区内执行，解决现有技术中的多次拷贝分段校验签名完成之后跳转到非安全的 FLASH 空间上执行代码期间的时间窗安全漏洞。

步骤 4：将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区进行签名校验，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot，签名校验成功后，执行步骤 5。

本发明实施例中，可以将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名一次性拷贝到 DDR 的安全区中。

签名校验的过程具体可以参见图 3。利用第二片外 Boot 的安全签名对第二片外 Boot 的代码进行签名验证，以验证第二片外 Boot 的代码是否被篡改过。

步骤 5：在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。

本发明实施例中，对第一片外 Boot 和第二片外 Boot 的校验签名和执行代码均在 SRAM 或者 DDR 的安全区进行，提高了系统启动过程的安全性。

通过实施本发明实施例，通过增加第一片外 Boot，在 SRAM 中在对第一片外 Boot 签名校验成功后，执行第一片外 Boot 的代码实现初始化 DDR 以及配置所述 DDR 安全区，进而将除第一片外 Boot 以外的其他所有片外 Boot 的签名校验以及执行代码的过程均在 DDR 安全区进行，避免了现有技术中先在 SRAM 安全区进行签名校验之后再跳转到非安全区的 FLASH 中执行代码期间的代码被篡改风险，提高了系统启动过程的安全性。

结合图 3，下面对签名校验过程进行介绍。

系统启动代码(系统的某个版本对应的启动代码，System Code)在进行启动时，需要先进行签名安全校验，以确保系统启动代码没有被篡改。图 3 为系统安全启动相关的签名校验过程示意图，图 3 所示的示意图中采用 eFuse 模块存储密钥等与安全相关的内容。

签名校验的原理可以为：采用基于 RSA 非对称加密算法，使用私钥签名，公钥校验的签名校验机制来构建安全启动的信任链。

芯片商随机生成非对称性密钥对，并将公钥 Hash 值和私钥指数烧入 Efuse，公钥写到 Flash 指定位置，设备商使用一单向散列函数：哈希(Hash)函数对系统启动代码生成信息摘要，然后使用 Efuse 私钥对信息摘要进行加密，即数字签名，签名后的信息摘要与系统启动代码放在一起，写到片外存储器，片外存储器通常是 FLASH，例如，图 2 中所示为非易失性随机访问存储器(Non-Volatile Random Access Memory，NVRAM)，公私钥对由芯片内部产生，烧写与校验过程不可见，且不备份。

安全启动时，系统由片内 Boot 启动，片内 Boot ROM 包含最小系统初始化和签名校验安全校验程序，先对 Flash 中的公钥生成 Hash 值，与 Efuse 的可信公钥根(Root Of Trust Public Key，ROTPK)比对，所述可信公钥根是安全启动使用的 EK 公钥(N，e)的 SHA256Hash 值，以保证校验签名使用的公钥是唯一指定的。如果通过则对片外系统启动代码生成 Hash 摘要值，再使用公钥校验签名得到原始 Hash 摘要值，对这两个信息摘要值进行校验，就知道系统启动代码是否被篡改过，是否是预期授权的代码。片外系统启动代码签名校验校验通过后，切换到片外系统启动代码执行，引导后续启动程序。

以上是对本发明实施例中的版本校验方法进行的介绍，下面对本发明实施例中的安全启动装置进行介绍。

请参见图 4，是本发明实施例提供的一种安全启动装置的结构示意图。如图 4 所示，安全启动装置 40 包括：拷贝单元 401、签名校验单元 402 和执行单元 403。

在本发明实施例中，拷贝单元 401，用于将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名拷贝到静态随机存储器 SRAM 中；

签名校验单元 402，用于对所述第一片外 Boot 的代码进行签名校验，所述第一片外 Boot 实现的功能包括初始化双倍速率同步动态随机存储器 DDR，所述初始化 DDR 过程包括配置 DDR 安全区；

执行单元 403，用于在所述签名校验单元 402 对所述第一片外 Boot 的代码进行签名校验成功后，在 SRAM 中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区；

拷贝单元 401，还用于将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot；

签名校验单元 402，还用于对所述第二片外 Boot 的代码进行签名校验；

执行单元 403，还用于在签名校验单元 402 对所述第二片外 Boot 的代码进行签名校验成功后，在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。

具体的，所述第一片外 Boot 为片外 Boot 中新增的一级 Boot。

具体的，所述第一片外 Boot 的容量小于或等于 SRAM 的容量。

需要说明的是，本发明实施例所描述的安全启动装置 40 中各功能模块的功能可参见上述图 2 所示实施例中的相关描述，此处不再赘述。

另外，本发明实施例还提供了一种芯片，该芯片用于执行程序代码，以执行上述安全启动方法实施例的全部或部分步骤。

此外，本发明实施例还提供了一种终端设备，该终端设备可以以一个用户设备(例如：手机)的形式存在。该终端设备还可以包括手持设备、车载设备、可穿戴设备、计算设备，以及各种形式的用户设备。手持设备可以为包括手机、平板电脑、PDA(Personal Digital Assistant，个人数字助理)、等任意终端设备。

请参见图 5，是本发明实施例提供的一种终端设备的结构示意图。参考图 5，终端设备 50 包括：射频(Radio Frequency，RF)电路 510、存储器 520、输入装置 530、输出装置 540、传感器 550、音频电路 560、无线保真(Wireless Fidelity，WiFi)模块 570、处理器 580、以及电源 590 等部件。其中，射频电路 510、WiFi 模块 570 为收发器。本领域技术人员可以理解，图 5 中示出的终端设备的结构并不构成对终端设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

下面结合图 5 对终端设备的各个构成部件进行具体的介绍：

存储器 520 可用于存储软件程序以及模块，处理器 580 通过运行存储在存储器 520 的软件程序以及模块，从而执行终端设备 50 的各种功能应用以及数据处理。存储器 520 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需

的应用程序(比如声音播放功能、图像播放功能等)等；存储数据区可存储根据终端设备 50 的使用所创建的 数据(比如音频数据、电话本等)等。此外，存储器 520 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器 件。

具体的，存储器 520 存储的应用程序为执行时包括上述图 2 所对应的方法中的部分或者全部步骤。存储器 520 中存储片外 Boot 的安全签名以及片外 Boot 的代码等信息。

输入单元 530 可用于接收输入的数字或字符信息，以及产生与终端设备 50 的用户设置以及功能控制有关的键信号输入。具体地，输入单元 530 可包括触控面板 531 以及其他输入设备 532。触控面板 531，也称为触摸屏，可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触控面板 531 上或在触控面板 531 附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触控面板 531 可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器 580，并能接收处理器 580 发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板 531。除了触控面板 531，输入单元 530 还可以包括其他输入设备 532。具体地，其他输入设备 532 可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

显示单元 540 可用于显示由用户输入的信息或提供给用户的信息。显示单元 540 可包括显示面板 541，可选的，可以采用液晶显示器(Liquid Crystal Display，LCD)、有机发光二极管(Organic Light-Emitting Diode,OLED)等形式来配置显示面板 541。进一步的，触控面板 531 可覆盖显示面板 541，当触控面板 531 检测到在其上或附近的触摸操作后，传送给处理器 580 以确定触摸事件的类型，随后处理器 580 根据触摸事件的类型在显示面板 541 上提供相应的视觉输出。虽然在图 5 中，触控面板 531 与显示面板 541 是作为两个独立的部件来实现终端设备 50 的输入和输入功能，但是在某些实施例中，可以将触控面板 531 与显示面板 541 集成而实现终端设备 50 的输入和输出功能。

处理器 580 是终端设备 50 的控制中心，利用各种接口和线路连接整个终端设备的各个部分，通过运行或执行存储在存储器 520 内的软件程序和/或模块，以及调用存储在存储器 520 内的数据，执行终端设备 50 的各种功能和处理数据，从而对终端设备 50 进行整体监控。可选的，处理器 580 可包括一个或多个处理单元；优选的，处理器 580 可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。 可以理解的是，上述调制解调处理器也可以不集成到处理器 580 中。

具体的，本发明实施例中的处理器 580 用于执行存储器 520 中的应用程序，以执行图 2 实施例中的处理器所执行的部分或者全部步骤。

终端设备 50 还可包括至少一种传感器 550、电源 590，尽管未示出，终端设备 50 还可以包括摄像头、蓝牙模块等，在此不再赘述。

另外，本发明实施例还提供了一种计算机存储介质，该介质存储有计算机软件程序指

令，该计算机软件程序指令被处理器执行时使所述处理器执行上述安全启动方法中的部分或者全部步骤。

结合本发明实施例公开内容所描述的方法或者算法的步骤可以硬件的方式来实现，也可以是由处理器执行软件程序指令的方式来实现。软件程序指令可以由相应的软件模块组成，软件模块可以被存放于 RAM、闪存、ROM、可擦除可编程只读存储器(Erasable Programmable ROM，EPROM)、电可擦可编程只读存储器(Electrically EPROM，EEPROM)、寄存器、硬盘、移动硬盘、只读光盘(CD-ROM)或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于终端设备中。

本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个程序指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

以上的具体实施方式，对本发明实施例的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上仅为本发明实施例的具体实施方式而已，并不用于限定本发明实施例的保护范围，凡在本发明实施例的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明实施例的保护范围之内。

权 利 要 求

1、一种安全启动方法，其特征在于，包括:

将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名拷贝到静态随机存储器 SRAM 中进行签名校验，所述第一片外 Boot 实现的功能包括初始化双倍速率同步动态随机存储器 DDR，所述初始化 DDR 过程包括配置 DDR 安全区;

在对所述第一片外 Boot 签名校验成功后，在 SRAM 中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区;

将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区进行签名校验，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot;

在对所述第二片外 Boot 签名校验成功后，在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。

2、根据权利要求 1 所述的方法，其特征在于，所述第一片外 Boot 为片外 Boot 中新增的一级 Boot。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一片外 Boot 的容量小于或等于 SRAM 的容量。

4、一种安全启动装置，其特征在于，包括:

拷贝单元，用于将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名拷贝到静态随机存储器 SRAM 中;

签名校验单元，用于对所述第一片外 Boot 的代码进行签名校验，所述第一片外 Boot 实现的功能包括初始化双倍速率同步动态随机存储器 DDR，所述初始化 DDR 过程包括配置 DDR 安全区;

执行单元，用于在所述签名校验单元对所述第一片外Boot的代码进行签名校验成功后，在 SRAM 中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区;

所述拷贝单元，还用于将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot;

所述签名校验单元，还用于对所述第二片外 Boot 的代码进行签名校验;

所述执行单元，还用于在所述签名校验单元对所述第二片外 Boot 的代码进行签名校验成功后，在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。

5、根据权利要求 4 所述的方法，其特征在于，所述第一片外 Boot 为片外 Boot 中新增的一级 Boot。

6、根据权利要求 4 或 5 所述的方法，其特征在于，所述第一片外 Boot 的容量小于或等于 SRAM 的容量。

7、一种终端设备，其特征在于，包括处理器和存储器，所述存储器用于存储程序指令和/或数据，所述处理器用于执行所述存储器中的程序指令和/或数据，执行如下操作：

将第一片外 Boot 的代码以及所述第一片外 Boot 的安全签名拷贝到静态随机存储器 SRAM 中进行签名校验，所述第一片外 Boot 实现的功能包括初始化双倍速率同步动态随机存储器 DDR，所述初始化 DDR 过程包括配置 DDR 安全区；

在对所述第一片外 Boot 签名校验成功后，在 SRAM 中执行所述第一片外 Boot 的代码，实现初始化 DDR 以及配置所述 DDR 安全区；

将第二片外 Boot 的代码以及所述第二片外 Boot 的安全签名拷贝到所述 DDR 的安全区进行签名校验，所述第二片外 Boot 是片外 Boot 中除所述第一片外 Boot 以外的其他全部 Boot；

在对所述第二片外 Boot 签名校验成功后，在所述 DDR 的安全区中执行所述第二片外 Boot 的代码。

8、根据权利要求 7 所述的方法，其特征在于，所述第一片外 Boot 为片外 Boot 中新增的一级 Boot。

9、根据权利要求 7 或 8 所述的方法，其特征在于，所述第一片外 Boot 的容量小于或等于 SRAM 的容量。

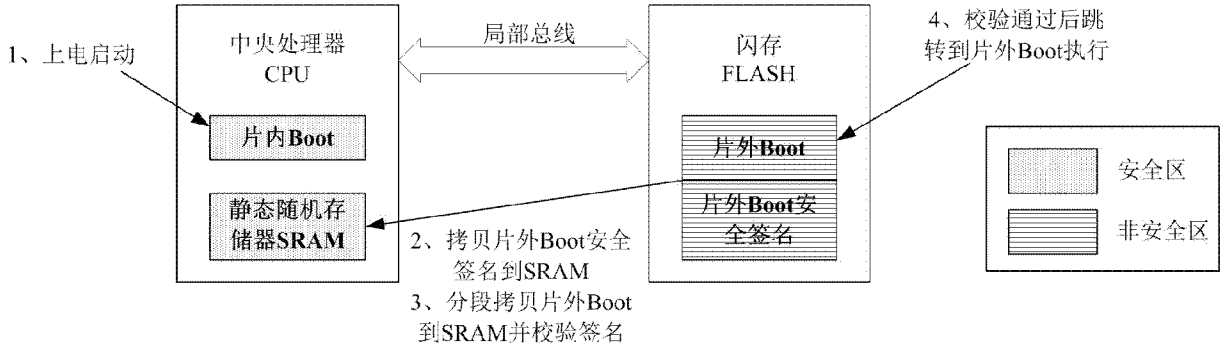
1、上电启动
中央处理器
CPU
片内Boot
静态随机存储器SRAM
局部总线
闪存
FLASH
片外Boot
片外Boot安全签名
2、拷贝片外Boot安全签名到SRAM
3、分段拷贝片外Boot到SRAM并校验签名
4、校验通过后跳转到片外Boot执行
安全区
非安全区

图 1

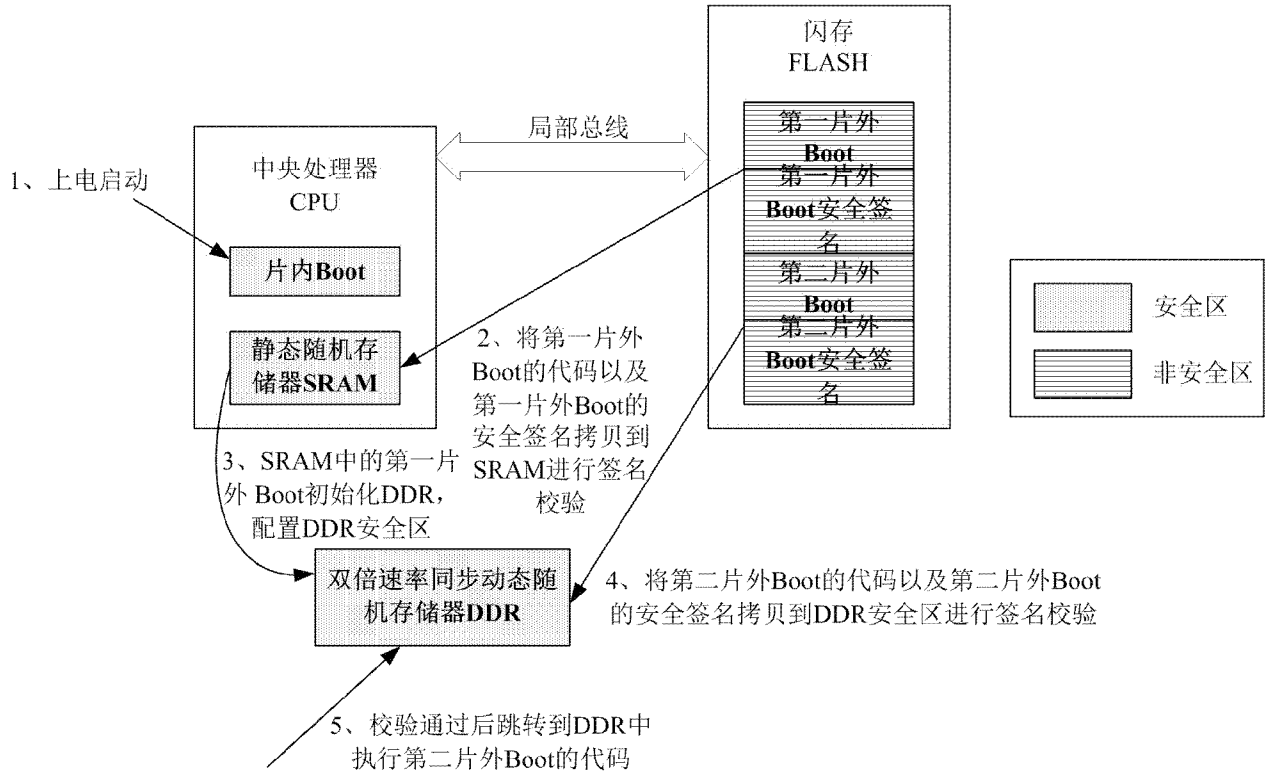
闪存
FLASH
局部总线
1、上电启动
中央处理器
CPU
片内Boot
静态随机存储器SRAM
第一片外Boot
第一片外Boot安全签名
第二片外Boot
第二片外Boot安全签名
2、将第一片外Boot的代码以及第一片外Boot的安全签名拷贝到SRAM进行签名校验
3、SRAM中的第一片外 Boot初始化DDR，配置DDR安全区
双倍速率同步动态随机存储器DDR
4、将第二片外Boot的代码以及第二片外Boot的安全签名拷贝到DDR安全区进行签名校验
5、校验通过后跳转到DDR中执行第二片外Boot的代码
安全区
非安全区

图 2

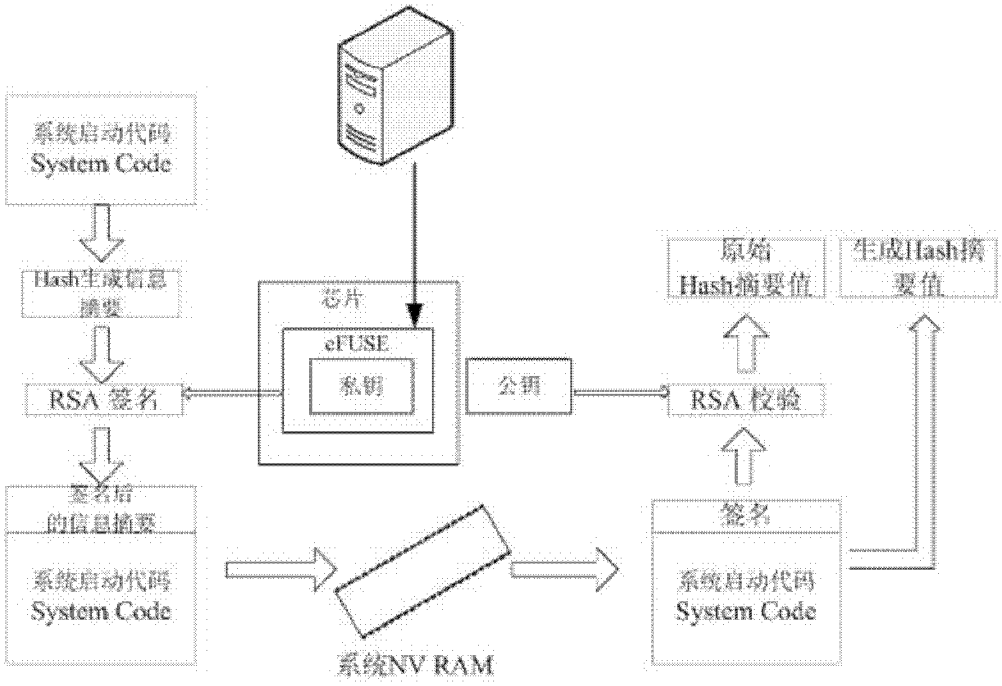
系统启动代码
System Code
Hash生成信息
摘要
RSA 签名
签名后
的信息摘要
系统启动代码
System Code
芯片
eFUSE
私钥
公钥
RSA 校验
原始
Hash摘要值
生成Hash摘
要值
签名
系统启动代码
System Code
系统NV RAM

图 3

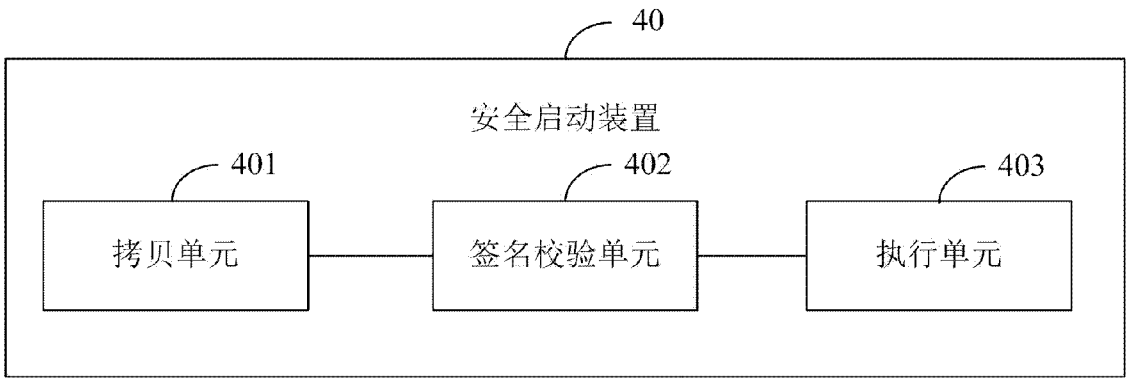
40
安全启动装置
401
拷贝单元
402
签名校验单元
403
执行单元

图 4

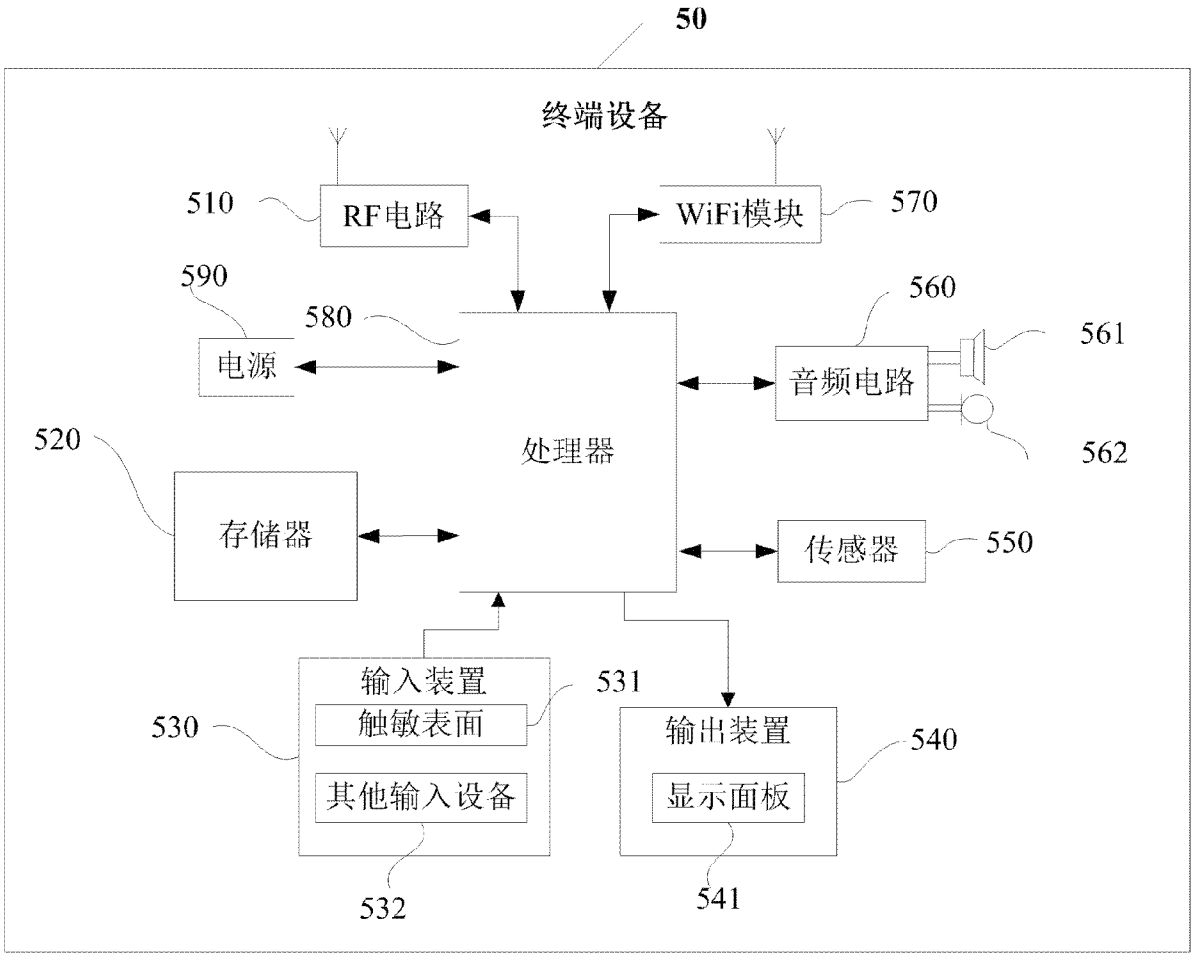
50
终端设备
510
RF电路
WiFi模块
570
590
580
560
561
电源
音频电路
处理器
562
520
存储器
传感器
550
输入装置
531
530
触敏表面
输出装置
540
其他输入设备
显示面板
532
541

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/108857

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)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; H04L

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)

CNPAT; CNKI; WPI; EPODOC: 启动, 安全, boot, 片上, 片外, 安全区, 闪存, 快闪, 静态随机存储器, 双倍速率同步动态随机存储器, drive, start, safe, secure, on chip, secure boot, trust zone, flash, SRAM, DDR

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103677912 A (HUAWEI TECHNOLOGIES CO., LTD.) 26 March 2014 (2014-03-26) description, paragraphs [0053]-[0091], and figures 3 and 4	1-9
A	CN 102388365 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 March 2012 (2012-03-21) entire document	1-9
A	US 2009113196 A1 (JAN, H.Y. ET AL.) 30 April 2009 (2009-04-30) entire document	1-9

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 November 2018	**04 January 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/108857

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 103677912 A	26 March 2014	US 2015160946 A1	11 June 2015
CN 102388365 A	21 March 2012	WO 2012149774 A1	08 November 2012
US 2009113196 A1	30 April 2009	TW 200919205 A	01 May 2009

国际检索报告

国际申请号
PCT/CN2018/108857

A. 主题的分类

G06F 21/57(2013.01)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; H04L

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）)

CNPAT;CNKI;WPI;EPODOC:启动，安全，boot，片上，片外，安全区，闪存，快闪，静态随机存储器，双倍速率同步动态随机存储器，drive，start，safe，secure，on chip，secure boot，trust zone，flash，SRAM，DDR

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103677912 A (华为技术有限公司) 2014年 3月 26日 (2014-03-26) 说明书第[0053]-[0091]段，图3、4	1-9
A	CN 102388365 A (华为技术有限公司) 2012年 3月 21日 (2012-03-21) 全文	1-9
A	US 2009113196 A1 (JAN HSUN-YAO等) 2009年 4月 30日 (2009-04-30) 全文	1-9

☐ 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	国际检索报告邮寄日期
2018年 11月 16日	2019年 1月 4日

ISA/CN的名称和邮寄地址	受权官员
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	陈希元
传真号 (86-10)62019451	电话号码 86-(10)-53961594

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/108857

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	103677912	A	2014年 3月 26日	US	2015160946	A1	2015年 6月 11日
CN	102388365	A	2012年 3月 21日	WO	2012149774	A1	2012年 11月 8日
US	2009113196	A1	2009年 4月 30日	TW	200919205	A	2009年 5月 1日