(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
2017 年 4 月 27 日 (27.04.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/067175 A1

(51) 国际专利分类号:
G06F 9/445 (2006.01)

(21) 国际申请号: PCT/CN2016/084304

(22) 国际申请日: 2016 年 6 月 1 日 (01.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510688388.3 2015 年 10 月 21 日 (21.10.2015) CN

(71) 申请人: **百度在线网络技术（北京）有限公司 (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.)** [CN/CN]; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。

(72) 发明人: **秦松 (QIN, Song)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **陈鑫 (CHEN, Xin)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **位广军 (WEI, Guangjun)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **马家智 (MA, Jiazhi)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **桂敬文 (GUI, Jingwen)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **王博通 (WANG, Botong)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **王晓卿 (WANG, Xiaoqing)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **张洪卫 (ZHANG, Hongwei)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **常磊 (CHANG, Lei)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **张治 (ZHANG, Zhi)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。 **李新开 (LI, Xinkai)**; 中国北京市海淀区上地十街 10 号百度大厦三层, Beijing 100085 (CN)。

(74) 代理人: **北京鸿德海业知识产权代理事务所（普通合伙） (BEIJING WISPRO INTELLECTUAL PROPERTY LLP.)**; 中国北京市海淀区知春路 6 号锦秋国际大厦 A508, Beijing 100088 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: METHOD, APPARATUS AND DEVICE FOR LOADING ELF FILE, AND COMPUTER STORAGE MEDIUM

(54) 发明名称 : 一种加载 ELF 文件的方法、装置、设备和计算机存储介质

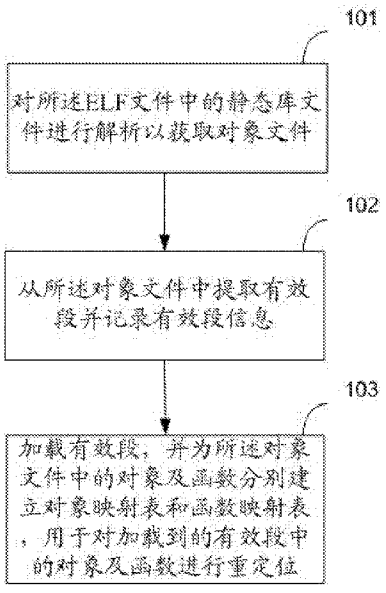


图 1

(57) Abstract: A method, apparatus and device for dynamically loading an executable and linking format (ELF) file, and a computer storage medium. The method comprises: parsing a static library file in an ELF file to obtain an object file (101); extracting an effective segment from the object file, and recording effective segment information (102); and loading the effective segment, and separately establishing an object mapping table and a function mapping table for objects and functions in the object file to re-position the objects and the functions in the loaded effective segment (103). By means of the method and device for dynamically loading an ELF file provided in the solution, the troubles of an embedded system needing to depend on a specific instruction set when the embedded system parses and loads an ELF file and the embedded system is not be suitable for all embedded processor architectures in the prior art can be eliminated, applications of multiple ELF files can be simultaneously operated under a specific processor system structure, and dynamic linking can be realized, thereby greatly reducing a file volume generated by using static linking before, and reducing power consumption.

(57) 摘要:

[见续页]

WO 2017/067175 A1

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))。

一种对具有可执行和链接格式（ELF）文件动态加载的方法、装置和计算机存储介质，其中方法包括：对所述 ELF 文件中的静态库文件进行解析以获取对象文件（101）；从所述对象文件中提取有效段并记录有效段信息（102）；加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载的有效段中的对象及函数进行重定位（103）。通过上述方案所提供的 ELF 文件动态加载的方法和装置，可以摆脱现有技术中嵌入式系统在解析和加载 ELF 文件时需要依赖于特定的指令集，无法适用于全部的嵌入式处理器架构的困扰，实现了在特定处理器体系结构下能够同时运行多个 ELF 文件的应用，并且能够实现动态链接，大大减小了之前采用静态链接产生的文件体积，减小了功耗。

一种加载 ELF 文件的方法、装置、设备和计算机存储介质

本申请要求了申请日为2015年10月21日，申请号为201510688388.3发明名称为“一种加载ELF文件的方法和装置”的中国专利申请的优先权。

技术领域

本发明涉及计算机领域，尤其涉及一种加载ELF文件的方法、装置、设备和计算机存储介质。

背景技术

具有可执行和链接格式的 ELF(Executable and Linking Format)是一种对象文件的格式，用于定义不同类型的对象文件(Object files)中的内容及其格式。由于现有的嵌入式操作系统对于 ELF 文件的加载采用的是静态链接的方式生成可执行文件，并采用烧录的方式将可执行文件直接烧录至内存（Flash）中，这些处理过程都必须在 ARM 指令集下完成的，而有些处理器采用的并非 ARM 指令集，且不支持其所采用的指令集到 ARM 指令集的切换，因此现有技术无法为此类处理器提供 ELF 文件的加载。

发明内容

本发明提出了一种加载 ELF 文件的方法、装置、设备和计算机存储介质，以便于解决现有技术在一些嵌入式系统中无法记载 ELF 文件的问题。

具体技术方案如下：

一种加载具有可执行和链接格式 ELF 文件的方法，所述方法包括：

对所述 ELF 文件中的静态库文件进行解析以获取对象文件；

从所述对象文件中提取有效段；

加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载的有效段中的对象及函数进行重定位。

根据本发明一优选实施例，提取的有效段包括：可执行代码段、应用数据段或重定位段。

根据本发明一优选实施例，根据所述对象文件的 ELF 文件头和段文件头表来提取有效段。

根据本发明一优选实施例，所述加载有效段包括：将不同类型的有效段分别加载到不同的区域。

根据本发明一优选实施例，所述将不同类型的有效段分别加载到不同的区域包括：

依照可执行代码段及相应重定位段的段信息，对可执行代码段进行重定位，将重定位后的可执行代码段写入 Flash；或者

依照应用数据段及相应重定位段的段信息，将应用数据段直接加载到 RAM。

根据本发明一优选实施例，所述段信息包括段序号、段偏移量或段大小。

根据本发明一优选实施例，所述可执行代码段包括.text 段，所述应用数据段包括.data 段、.bss 段、或.rodata 段，所述重定位段包括.rel.data 段、.rel.bss 段、或.rel.rodata 段。

根据本发明一优选实施例，在所述加载有效段之后，对所述对象文件的有效段进行以下至少一个的标记：段的起始地址、段偏移量、段大小。

根据本发明一优选实施例，所述对象映射表的映射表项包括对象名

称和对象地址，所述对象地址是通过查找有效段中的导出对象，根据导出对象所在地址而得到的；所述函数映射表的映射表项包括函数名称和函数地址，所述函数地址是通过查找有效段中的导出函数，根据导出函数所在的地址而得到的。

根据本发明一优选实施例，在对有效段中的对象进行重定位时，利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

根据本发明一优选实施例，在对有效段中的函数进行重定位时，利用当前函数运行时的地址以及从函数映射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

一种加载 ELF 文件的装置，所述装置包括：

解析装置，用于对所述 ELF 文件中的静态库文件进行解析以获取对象文件；

提取装置，用于从所述对象文件中提取有效段；

加载装置，用于加载有效段，为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，并且用于对加载的有效段中的对象及函数进行重定位。

根据本发明一优选实施例，所述提取装置中提取的有效段包括：可执行代码段、应用数据段或重定位段。

根据本发明一优选实施例，所述提取装置用于根据所述对象文件的 ELF 文件头和段文件头表来提取有效段。

根据本发明一优选实施例，所述加载装置加载有效段包括：将不同类型的有效段分别加载到不同的区域。

根据本发明一优选实施例，所述加载装置在将不同类型的有效段分别加载到不同的区域时，具体执行：

依照可执行代码段及相应重定位段的段信息，对可执行代码段进行重定位，将重定位后的可执行代码段写入 Flash；或者

依照应用数据段及相应重定位段的段信息，将应用数据段直接加载到 RAM。

根据本发明一优选实施例，所述段信息包括段序号、段偏移量或段大小。

根据本发明一优选实施例，所述可执行代码段包括.text 段，所述应用数据段包括.data 段、.bss 段、或.rodata 段，所述重定位段包括.rel.data 段、.rel.bss 段、或.rel.rodata 段。

根据本发明一优选实施例，所述加载装置在执行所述加载有效段之后，进一步用于对所述对象文件的有效段进行以下至少一个的标记：段的起始地址、段偏移量、段大小。

根据本发明一优选实施例，所述对象映射表的映射表项包括对象名称和对象地址，所述对象地址是通过查找有效段中的导出对象，根据导出对象所在地址而得到的；所述函数映射表的映射表项包括函数名称和函数地址，所述函数地址是通过查找有效段中的导出函数，根据导出函数所在的地址而得到的。

根据本发明一优选实施例，所述加载装置在对有效段中的对象进行重定位时，具体执行：

利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

根据本发明一优选实施例，所述加载装置在对有效段中的函数进行重定位时，具体执行：利用当前函数运行时的地址以及从函数映射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

由以上技术方案可以看出，本发明采用了解析静态库（.a）文件并且提取有效段，对有效段进行加载，建立对象及函数映射表用于对可重定位段中的对象和函数分别进行重定位的方式，这些处理方式并不受限于特定指令集，因此解决了现有技术在一些嵌入式系统中无法加载 ELF 文件的问题。

附图说明

图 1 为本发明实施例提供的一种对 ELF 文件动态加载方法的流程示意图；

图 2 为本发明实施例提供的 ELF Header 的格式示意图；

图 3 为本发明实施例提供的一种加载 ELF 文件的装置的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

请参考图 1，图 1 为本发明提供的一种加载具有可执行和链接格式的 ELF 文件的方法实施例的流程示意图。如图 1 所示，该流程包括：

101: 对 ELF 文件中的静态库(.a)文件进行解析以获取对象文件(.o)。

本发明的对象文件（.o）是以 ELF 格式保存的可重定向文件，对象文件中的内容可以包含对各个函数的入口标记，描述，以形成机器可执行的指令。当程序要执行时还需要进行链接(link)，链接就是把多个.o 文件链成一个可执行文件。

ELF 文件除了可以包含可重定位的对象文件外，还可以包含可执行的对象文件和可被共享的对象文件，上述三种对象文件由于都可以以对象文件.o 的形式表示，而多个 .o 对象文件可以归档(archive)成 .a 静态库文件，从而最终组成 ELF 文件，因此本发明中解析静态库（.a）文件的目的就是为了获取组成 ELF 文件的对象文件（.o）。

具体地，解析静态库文件的过程与 windows 操作系统中一个压缩包 rar 的解压缩（还原）过程类似，也就是分析由对象文件（.o）打包生成的静态库（.a），解析其中每个对象文件（.o）。

102: 从获取的对象文件中提取有效段（section）。

当获取对象文件（.o）后，可以针对每一个对象文件，从中提取有效段并且记录段信息。

有效段(sections)在 ELF 文件里面，用以装载内容数据的最小容器。

优选地，可以针对每个获取的对象文件，根据所述对象文件的 ELF 文件头（ELF Header）和段文件头表（SHT，Section Header Table）来提取有效段并记录各段信息。

该有效段的具体类型可以包括：可执行代码段，应用数据段，或重定位段。其中该可执行代码段又可以具体包括.text 段等，该应用数据段可以包括.data 段、.bss 段、或.rodata 段等，该重定位段可以包括.rel.data

段、.rel.bss 段、或 rel.rodata 段等。

该记录的有效段信息包括但不限于：各段序号、段偏移量、或段大小等。

其中

1) .text 段里装载了可执行代码;

2) .data 段里装载了被初始化的数据;

3) .bss 段里装载了未被初始化的数据;

4）.rodata 段里装载了相应字符串和定义的常量

5) 以.rel 打头的重定位段 rel.text 段、.rel.data 段、.rel.bss 段、.rel.rodata 段里面装载了重定位条目，该重定位段是用于帮助可执行代码段和应用数据段进行重定位的段;

例如：.rel.text 中示出了.text 段中哪些地方需要做重定位。

以下举个具体实例以说明从对象文件的 ELF Header 和 SHT 中提取有效段及各段信息的具体方式:

本实施例中的 ELF Header 可以以图 2 所示的格式表示。

如图 2 所示，该 ELF Header 表示了可重定位对象文件(.o)的格式。可以从该 ELF Header 中得知相应的 sections 及序号，而一个 ELF 文件中到底有哪些具体的 sections，则反映在这个 ELF 文件中的 SHT 中。

SHT 表中条目的结构定义可以为:

```
typedef struct {
Elf32_Word      sh_name;
Elf32_Word      sh_type;
Elf32_Word      sh_flags;
```

```
Elf32_Addr      sh_addr;
Elf32_Off       sh_offset;
Elf32_Word      sh_size;
Elf32_Word      sh_link;
Elf32_Word      sh_info;
Elf32_Word      sh_addralign;
Elf32_Word      sh_entsize;
} Elf32_Shdr;
```

在 SHT 中，针对每一个 section，都设置有一个条目，用来描述对应的这个 section，其内容主要包括该 section 的名称、类型、大小以及在整个 ELF 文件中的字节偏移位置等等。

上述 SHT 表中条目的结构中字段 Off(sh_offset)表示了该 section 离开文件头部位置的距离，即偏移量；Size(sh_size)表示 section 的段大小。

从而根据 ELF Header 和 SHT 表示的相关 section 从而能够提取各有效段的信息。

以上的 101 和 102 是在动态加载 ELF 文件之前对加载的准备过程，其步骤可以同时或者分先后执行，本发明对其执行的顺序不做硬性规定，当上述准备过程执行后，则通过 103 进一步实现对对象文件的有效段的加载。

103：加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载到的有效段中的对象及函数进行重定位。

对于 103，还可以将其进一步划分为加载有效段、建立映射表以及

重定位三个步骤，其中前两个步骤可以同时或者分先后执行，本发明对其执行的顺序不做硬性规定，只要能完成相应的功能，则均在本发明保护范围之内。

以下对三个步骤进行详细描述:

第一步：加载有效段。

对于在 102 所提取的有效段，包括可执行代码段、应用数据段以及重定位段三种类型，其中可执行代码段和应用数据段属于需要加载的有效段，而重定位段不需要加载，针对该需要加载的有效段，可以依据其类型的不同可以对应的采用两种方式将其加载到不同的区域。

第一种方式，对于可执行代码段（.text 段）加载:

由于针对于不同的产品其 flash 的读写不一致，因此为了便于重定位修改.text 段内容，可以先对.text 段进行重定位，然后再将其写入 Flash。

由于提取的与.text 段相应的重定位段（.rel.text 段）中包含.text 段需要重定位的信息，因此在写入 flash 之前的重定位方式可以为：将识别出的.rel.text 段中记录的.text 段需要重定位的部分记录下来创建重定位信息，对.text 做重定位，然后再将.text 段拷贝并写入到 Flash 中。

第二种方式，对于应用数据段（.data、.bss 及.rodata）的加载:

对于.data、.bss 及.rodata 的加载方式与对.text 段的加载方式略有不同，相比于对.text 段的加载在写入到 Flash 之前还包括对.text 段的重定位过程而言，对.data、.bss 及.rodata 的加载在将各段加载到随机存取存储器（Random Access Memory，RAM）之前并不需要进行重定位，而是依照.data、.bss 及.rodata 及相应重定位段(..rel.data、.rel.bss 及.rel.rodata）的有效段信息,将.data、.bss 及.rodata 段直接加载到 RAM。

在通过第一种和第二种方式加载有效段后，可以对各个对象文件（.o）的各个段做好相应的标记，该标记可以包括但不限于段的起始地址、段偏移量、段大小等信息。

其中段的起始地址是根据对加载后的有效段初始化获得的，段偏移量、段大小是在提取有效段时基于该提取的有效段获得的。

在第一步中，通过将装载了可执行代码的.text 段与其他的应用数据段的应用数据分离，并通过对可执行代码的目标文件创建重定位信息并载入内存，从而生成内存映射过程，避免了在加载 ELF 文件时多次拷贝代码数据的过程，提高了运行效率。

第二步，为对象文件中的对象及函数分别建立对象映射表和函数映射表。

在本步骤中，按照对象及函数的区别分别建立对象映射表（obj_map）及函数映射表（func_map），所建立的映射表供后续重定位及外部调用使用。

其中对象映射表的映射表项包括对象名称和对象地址，该映射表中的对象地址是通过查找对象文件的有效段中的导出对象，根据导出对象所在地址而得到的；函数映射表的映射表项包括函数名称和函数地址，该函数地址是通过查找对象文件的有效段中的导出函数，根据导出函数所在的地址而得到的。

关于对象和函数，举个例子：其中.text 段中包含的大部分为函数，而.text 段、.data 段、.bss 段、.rodata 段中文件变量、函数变量等全局变量、函数元素等都可以以对象表示。由于对象和函数的划分为现有技术，在此不再赘述。

第三步，对加载到的有效段中的对象及函数进行重定位。

在本步骤中，使用对象映射表对有效段中的对象进行重定位，或使用所述函数映射表对有效段中的函数进行重定位。

具体地，在链接时，需要对所有目标文件的可重定位段进行重定位，建立符号引用规则，同时为对象，函数等分配地址。程序执行时，把代码加载到链接时指定的地址空间，以保证程序在执行过程中对对象，函数等符号的正确引用，使程序正常运行。

基于对象文件中提取出的对象及函数类型的不同，可以采用两种不同的重定位方式。

第一种方式，对对象（obj）进行重定位:

对象在.o 文件中的使用方式是，直接将对象的真实地址写入文字池。在动态加载此对象时，利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

具体地，编译器会把对象的地址都放到文字池（Literal Pool）区域。其中 Literal Pool 里面只存放绝对地址或常量。当需要进行重定位时，根据.rel.text、.rel.data、.rel.bss 及.rel.rodata 所包含的对象重定位信息，通过对象映射表中所记录的对象的当前地址获取文字池中所记录的跳转对象的绝对地址，从 Literal Pool 中查找绝对地址，在动态加载时，将对象所在的文字池中的绝对地址修改为当前对象所在的地址，从而对.text、.data、.bss 及.rodata 段包含的对象做重定位。

第二种方式，对函数（func）进行重定位:

对于函数的重定位，可以利用当前函数运行时的地址以及从函数映

射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

具体地，函数调用跳转采用相应的跳转指令，例如 B/BL 等，对函数进行重新定位时，基于.rel.text 等所包含的函数重定位信息，从函数映射表中查找需要跳转到的函数的真实地址，根据函数运行时所在的当前地址结合从函数映射表中查找到的需要跳转到的函数真实地址，经过一系列计算得到跳转指令，获取正确的跳转指令对之前的跳转指令进行更新，从而根据更新后的跳转指令加载重定位的函数。

当然，并非只能依据对象映射表和函数映射表来查找地址，由于动态加载时对象可能引用的是外部对象或者函数使用的是动态库函数，因此当在对象或函数映射表中无法找到相应的地址信息时，则表明对象或函数引用的是外部对象或者动态库函数，此时可以去动态的查找对象或函数的地址以便重定位，从而实现动态加载。

请参考图 3，图 3 为本发明提供的一种加载 ELF 文件的装置实施例的结构示意图。如图 3 所示，该装置包括：解析装置 301，提取装置 302 和加载装置 303，以下对各装置进行详细描述：

解析装置 301，用于对 ELF 文件中的静态库（.a）文件进行解析以获取对象文件（.o）。

本发明的对象文件（.o）是以 ELF 格式保存的可重定向文件，对象文件中的内容可以包含对各个函数的入口标记，描述，以形成机器可执行的指令。当程序要执行时还需要进行链接(link)，链接就是把多个.o 文件链成一个可执行文件。多个 .o 对象文件可以归档(archive)成 .a 静态

库文件，而静态库文件行成了 ELF 文件。

其中解析装置解析静态库（.a）文件的目的是为了获取其中的对象文件（.o）。

具体地，解析静态库文件的过程与 windows 操作系统中一个压缩包 rar 的解压缩（还原）过程类似，也就是分析由对象文件（.o）打包生成的静态库（.a），解析其中每个对象文件（.o）。

提取装置 302，用于从获取的对象文件中提取有效段（section）。

当获取对象文件（.o）后，可以针对每一个对象文件，从中提取有效段并且记录段信息。

有效段(sections)在 ELF 文件里面，用以装载内容数据的最小容器。在 ELF 文件里，每一个 sections 内都装载了性质属性相同的内容。，

优选地，可以针对每个获取的对象文件，根据所述对象文件的 ELF 文件头（ELF Header）和段文件头表（SHT，Section Header Table）来提取有效段并记录各段信息。

该有效段的具体类型可以包括：可执行代码段，应用数据段，或重定位段。其中该可执行代码段又可以具体包括.text 段等，该应用数据段可以包括.data 段、.bss 段、或.rodata 段等，该重定位段可以包括.rel.data 段、.rel.bss 段、或 rel.rodata 段等。

该记录的有效段信息包括但不限于：各段序号、段偏移量、或段大小等。

其中

1) .text 段里装载了可执行代码;

2) .data 段里装载了被初始化的数据;

3) .bss 段里装载了未被初始化的数据;

4）.rodata 段里装载了相应字符串和定义的常量

5) 以.rel 打头的重定位段 rel.text 段、.rel.data 段、.rel.bss 段、.rel.rodata 段里面装载了重定位条目，该重定位段是用于帮助可执行代码段和应用数据段进行重定位的段;

例如: .rel.text 中示出了.text 段中哪些地方需要做重定位。

从对象文件的 ELF Header 和 SHT 中提取有效段及各段信息的具体方式可以为:

从 ELF Header 中得知相应的 sections 及序号，从 SHT 的内容中，根据 SHT 中的字段 Off(sh_offset)、Size(sh_size)来获取段偏移量、段大小等信息。

装置 301 和 302 用于在动态加载 ELF 文件之前对预加载的 ELF 文件执行加载前的准备，其准备过程可以同时或者分先后执行，本发明对其执行的顺序不做硬性规定，当上述准备过程执行后，则通过装置 303 进一步实现对对象文件的有效段的加载。

加载装置 303，用于加载有效段，为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，并且用于对加载到的有效段中的对象及函数进行重定位。

还可以将加载装置 303 进一步划分为有效段加载单元 3031、映射表建立单元 3032 以及重定位单元 3033 三个单元，其中前两个单元可以同时或者分先后执行相应操作，本发明对其执行的顺序不做硬性规定，只要能完成相应的功能，则均在本发明保护范围之内。

以下对三个单元进行详细描述:

加载有效段单元 3031。

对于由提取单元 302 所提取的有效段，包括可执行代码段、应用数据段以及重定位段三种类型，其中可执行代码段和应用数据段属于需要加载的有效段，而重定位段不需要加载，针对该需要加载的有效段，可以依据其类型的不同可以对应的采用两种方式将其加载到不同的区域。

第一种方式，对于可执行代码段（.text 段）加载:

由于针对于不同的产品其 flash 的读写不一致，因此为了便于重定位修改.text 段内容，可以先对.text 段进行重定位，然后再将其写入 Flash。

由于提取的与.text 段相应的重定位段（.rel.text 段）中包含.text 段需要重定位的信息，因此在写入 flash 之前的重定位方式可以为：将识别出的.rel.text 段中记录的.text 段需要重定位的部分记录下来创建重定位信息，对.text 做重定位，然后再将.text 段拷贝并写入到 Flash 中。

第二种方式，对于应用数据段（.data、.bss 及.rodata）的加载:

对于.data、.bss 及.rodata 的加载方式与对.text 段的加载方式略有不同，相比于对.text 段的加载在写入到 Flash 之前还包括对.text 段的重定位过程而言，对.data、.bss 及.rodata 的加载在将各段加载到随机存取存储器（Random Access Memory，RAM）之前并不需要进行重定位，而是依照.data、.bss 及.rodata 及相应重定位段（.rel.data、.rel.bss 及.rel.rodata）的有效段信息,将.data、.bss 及.rodata 段直接加载到 RAM。

在通过第一种和第二种方式加载有效段后，可以对各个对象文件（.o）的各个段做好相应的标记，该标记可以包括但不限于段的起始地址、段偏移量、段大小等信息。

其中段的起始地址是根据对加载后的有效段初始化获得的，段偏移

量、段大小是在提取有效段时基于该提取的有效段获得的。

本实施例通过加载有效段单元的操作，将装载了可执行代码的.text段与其他的应用数据段的应用数据分离，并通过对可执行代码的目标文件创建重定位信息并载入内存，从而生成内存映射过程，避免了在加载ELF文件时多次拷贝代码数据的过程，提高了运行效率。

映射表建立单元3032，用于为对象文件中的对象及函数分别建立对象映射表和函数映射表。

本单元用于按照对象及函数的区别分别建立对象映射表（obj_map）及函数映射表（func_map），所建立的映射表供后续重定位及外部调用使用。

其中对象映射表的映射表项包括对象名称和对象地址，该映射表中的对象地址是通过查找对象文件的有效段中的导出对象，根据导出对象所在地址而得到的；函数映射表的映射表项包括函数名称和函数地址，该函数地址是通过查找对象文件的有效段中的导出函数，根据导出函数所在的地址而得到的。

关于对象和函数，举个例子：其中.text段中包含的大部分为函数，而.text段、.data段、.bss段、.rodata段中文件变量、函数变量等全局变量、函数元素等都可以以对象表示。由于对象和函数的划分为现有技术，在此不再赘述。

重定位单元3033，用于对加载到的有效段中的对象及函数进行重定位。

本单元用于使用对象映射表对有效段中的对象进行重定位，或使用所述函数映射表对有效段中的函数进行重定位。

具体地，在链接时，需要对所有目标文件的可重定位段进行重定位，建立符号引用规则，同时为对象，函数等分配地址。程序执行时，把代码加载到链接时指定的地址空间，以保证程序在执行过程中对对象，函数等符号的正确引用，使程序正常运行。

基于对象文件中提取出的对象及函数类型的不同，可以采用两种不同的重定位方式。

第一种方式，对对象（obj）进行重定位:

对象在.o 文件中的使用方式是，直接将对象的真实地址写入文字池。在动态加载此对象时，利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

第二种方式，对函数（func）进行重定位:

对于函数的重定位，可以利用当前函数运行时的地址以及从函数映射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

当然，并非只能依据对象映射表和函数映射表来查找地址，由于动态加载时对象可能引用的是外部对象或者函数使用的是动态库函数，因此当在对象或函数映射表中无法找到相应的地址信息时，则表明对象或函数引用的是外部对象或者动态库函数，此时可以查找对象或函数的地址以便重定位，从而实现动态加载。

本发明的 ELF 文件动态记载的方式和装置，可以应用于机顶盒、智能可穿戴式设备、智能家居云等多种场景中。以机顶盒为例，当用户使

用机顶盒启动或者安装 ELF 文件时，可以使用本发明所提供的方法和装置，通过对静态库文件（.a）进行解析并进行加载和重定位，从而实现 ELF 文件的动态加载。

本发明提供的方法和装置可以具备下优点：

1）本发明采用了解析静态库（.a）文件并且提取有效段，对有效段进行加载，建立对象及函数映射表用于对可重定位段中的对象和函数分别进行重定位的方式，这些处理方式并不受限于特定指令集，因此解决了现有技术在一些嵌入式系统中无法加载 ELF 文件的问题。

举一个例子，本发明尤其适用于支持采用 Thumb-2 指令集的 Cortex-M 系列处理器嵌入式系统。由于嵌入式 Mbed OS 是基于 ARM Cortex-M 处理器所设计的操作系统，Mbed os 作为专门为嵌入式开发定制的系统具有独特的优势。目前 Cortex-M 系列处理器已经能够支持 Mbed os，但目前 Mbed os 还无法提供适用于 Cortex-M 处理器的 ELF 文件加载器（Loader），因此限制了 Mbed os 在 Cortex-M 系列处理器上的使用。这是因为现有的嵌入式操作系统对于 ELF 文件的加载采用静态链接的方式生成可执行文件，并将可执行文件烧录至 Flash，这些操作都必须在 ARM 指令集下完成，但是由于 Cortex-M 系列处理器指令集采用的是 Thumb-2 指令集，该指令集不支持切换到 ARM 指令集的状态，因此现有技术无法为此类处理器提供动态解析加载 ELF 文件的加载器。

而本发明提供的方法和装置转换了一种思路，不是通过静态链接的方式生成可执行文件并直接载入内存的方式，也不需要通过特定的 ARM 指令集来解析和加载 ELF 文件。而是对 ELF 文件的静态库文件进行解析

以获取 ELF 可重定位的对象文件的有效段并进行重定位，以便使 ELF 文件中的对象及函数能够以可重定位的方式被动态加载。本发明的这些处理过程并不受限于特定的 ARM 指令集，因此尤其适用于支持采用 Thumb-2 指令集的 Cortex-M 系列处理器嵌入式系统。

2）现有技术中采用静态链接的方式生成可执行文件，并将可执行文件烧录至 Flash，因此其运行的应用数量受限于 Flash 中烧录的可执行文件数量。而本发明采用动态加载方式，基于此能够实现动态链接，运行的应用数量不再受限于 Flash 中烧录可执行文件数量。

3）静态链接的方式需要生成可执行文件并载入 Flash，这就造成了文件体积较大，功耗较大。本申请的动态加载方式相比较现有技术大大较小了文件体积和功耗。

在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

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。

权 利 要 求 书

1.一种加载具有可执行和链接格式 ELF 文件的方法，其特征在于，所述方法包括:

对所述 ELF 文件中的静态库文件进行解析以获取对象文件;

从所述对象文件中提取有效段;

加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载的有效段中的对象及函数进行重定位。

2.根据权利要求 1 所述的方法，其特征在于，提取的有效段包括:可执行代码段、应用数据段或重定位段。

3.根据权利要求 1 或 2 所述的方法，其特征在于，根据所述对象文件的 ELF 文件头和段文件头表来提取有效段。

4.根据权利要求 1 或 2 所述的方法，其特征在于，所述加载有效段包括：将不同类型的有效段分别加载到不同的区域。

5.根据权利要求 4 所述的方法，其特征在于，所述将不同类型的有效段分别加载到不同的区域包括:

依照可执行代码段及相应重定位段的段信息，对可执行代码段进行重定位，将重定位后的可执行代码段写入 Flash；或者

依照应用数据段及相应重定位段的段信息，将应用数据段直接加载到 RAM。

6.根据权利要求 5 所述的方法，其特征在于，所述段信息包括段序号、段偏移量或段大小。

7.根据权利要求 5 所述的方法，其特征在于，所述可执行代码段包括.text 段，所述应用数据段包括.data 段、.bss 段、或.rodata 段，所述重

定位段包括.rel.data 段、.rel.bss 段、或.rel.rodata 段。

8.根据权利要求 1 或 2 所述的方法，其特征在于，在所述加载有效段之后，对所述对象文件的有效段进行以下至少一个的标记：段的起始地址、段偏移量、段大小。

9.根据权利要求 1 所述的方法，其特征在于：

所述对象映射表的映射表项包括对象名称和对象地址，所述对象地址是通过查找有效段中的导出对象，根据导出对象所在地址而得到的；

所述函数映射表的映射表项包括函数名称和函数地址，所述函数地址是通过查找有效段中的导出函数，根据导出函数所在的地址而得到的。

10.根据权利要求 1 所述的方法，其特征在于，在对有效段中的对象进行重定位时，利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

11.根据权利要求 1 所述的方法，其特征在于，在对有效段中的函数进行重定位时，利用当前函数运行时的地址以及从函数映射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

12. 一种加载 ELF 文件的装置，其特征在于，所述装置包括：

解析装置，用于对所述 ELF 文件中的静态库文件进行解析以获取对象文件；

提取装置，用于从所述对象文件中提取有效段；

加载装置，用于加载有效段，为所述对象文件中的对象及函数分别

建立对象映射表和函数映射表，并且用于对加载的有效段中的对象及函数进行重定位。

13.根据权利要求 12 所述的加载 ELF 文件的装置，其特征在于，所述提取装置中提取的有效段包括：可执行代码段、应用数据段或重定位段。

14.根据权利要求 12 或 13 所述的加载 ELF 文件的装置，其特征在于，所述提取装置用于根据所述对象文件的 ELF 文件头和段文件头表来提取有效段。

15.根据权利要求 12 或 13 所述的加载 ELF 文件的装置，其特征在于，所述加载装置加载有效段包括：将不同类型的有效段分别加载到不同的区域。

16.根据权利要求 15 所述的加载 ELF 文件的装置，其特征在于，所述加载装置在将不同类型的有效段分别加载到不同的区域时，具体执行：

依照可执行代码段及相应重定位段的段信息，对可执行代码段进行重定位，将重定位后的可执行代码段写入 Flash；或者

依照应用数据段及相应重定位段的段信息，将应用数据段直接加载到 RAM。

17.根据权利要求 16 所述的加载 ELF 文件的装置，其特征在于，所述段信息包括段序号、段偏移量或段大小。

18.根据权利要求 16 所述的加载 ELF 文件的装置，其特征在于，所述可执行代码段包括.text 段，所述应用数据段包括.data 段、.bss 段、或.rodata 段，所述重定位段包括.rel.data 段、.rel.bss 段、或.rel.rodata 段。

19.根据权利要求 12 或 13 所述的加载 ELF 文件的装置，其特征在于，

所述加载装置在执行所述加载有效段之后，进一步用于对所述对象文件的有效段进行以下至少一个的标记：段的起始地址、段偏移量、段大小。

20.根据权利要求 12 所述的加载 ELF 文件的装置，其特征在于：

所述对象映射表的映射表项包括对象名称和对象地址，所述对象地址是通过查找有效段中的导出对象，根据导出对象所在地址而得到的；

所述函数映射表的映射表项包括函数名称和函数地址，所述函数地址是通过查找有效段中的导出函数，根据导出函数所在的地址而得到的。

21.根据权利要求 12 所述的加载 ELF 文件的装置，其特征在于，所述加载装置在对有效段中的对象进行重定位时，具体执行：

利用当前对象在所述对象映射表中的地址查找所述对象的跳转对象在文字池中的地址，并将文字池中所述跳转对象的地址修改为当前对象的地址。

22.根据权利要求 12 所述的加载 ELF 文件的装置，其特征在于，所述加载装置在对有效段中的函数进行重定位时，具体执行：利用当前函数运行时的地址以及从函数映射表中查找到的需要跳转到的函数地址，经过计算得到跳转指令，利用计算得到的跳转指令对之前的跳转指令进行更新，以便于根据所述更新的跳转指令跳转到即将要执行的函数地址。

23.一种设备，包括

一个或者多个处理器；

存储器；

一个或者多个程序，所述一个或者多个程序存储在所述存储器中，当被所述一个或者多个处理器执行时：

对所述 ELF 文件中的静态库文件进行解析以获取对象文件；

从所述对象文件中提取有效段；

加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载的有效段中的对象及函数进行重定位。

24.一种计算机存储介质，所述计算机存储介质被编码有计算机程序，所述程序在被一个或多个计算机执行时，使得所述一个或多个计算机执行如下操作：

对所述 ELF 文件中的静态库文件进行解析以获取对象文件；

从所述对象文件中提取有效段；

加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载的有效段中的对象及函数进行重定位。

说明书附图

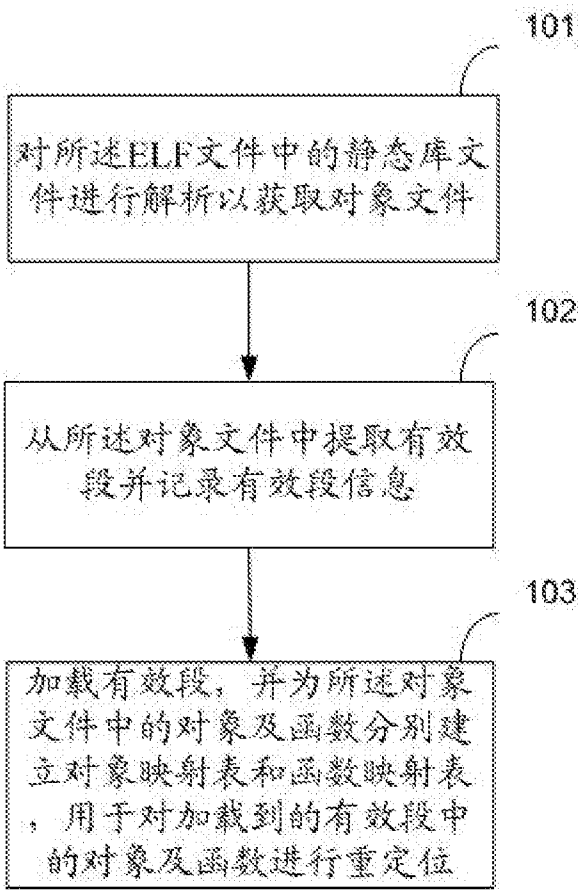

101
对所述ELF文件中的静态库文件进行解析以获取对象文件
102
从所述对象文件中提取有效段并记录有效段信息
103
加载有效段，并为所述对象文件中的对象及函数分别建立对象映射表和函数映射表，用于对加载到的有效段中的对象及函数进行重定位

图 1

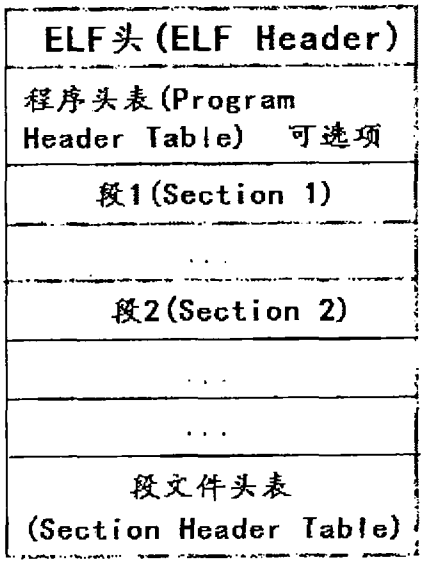

ELF头(ELF Header)
程序头表(Program Header Table) 可选项
段1(Section 1)
...
段2(Section 2)
...
...
段文件头表 (Section Header Table)

图 2

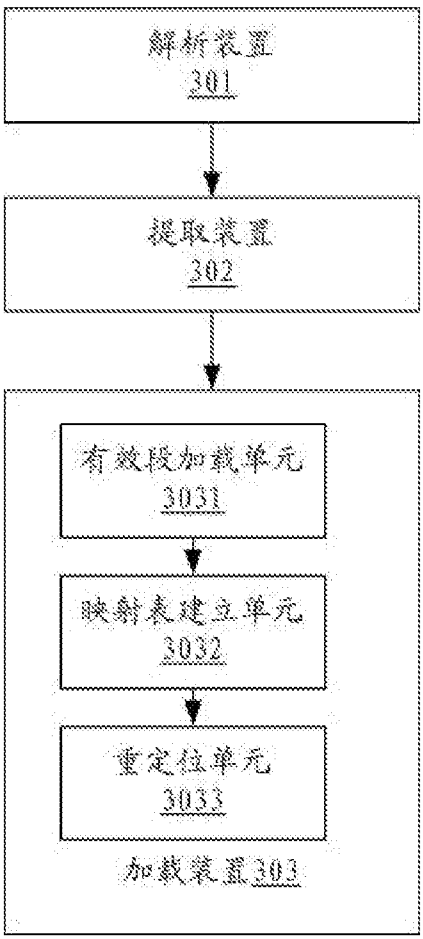

解析装置
301
提取装置
302
有效段加载单元
3031
映射表建立单元
3032
重定位单元
3033
加载装置303

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/084304

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; 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)

WPI, EPODOC, CNPAT, CNKI: ELF, executable and linking format, linux, unix, kernel, function address, dynamic, static, map+, object, load, ARM, x86

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105224370 A (ANYIHENGTONG (BEIJING) TECHNOLOGY CO., LTD.), 06 January 2016 (06.01.2016), claims 1-22	1-24
X	emmoblin, "Understanding of Executable and Linking Format, URL:blog.chinaunix.net/uid-20778443-id-99714.html", 20010123, pages 1-7	1-24
A	CN 101697131 A (ZTE CORP.), 21 April 2010 (21.04.2010), the whole document	1-24
A	CN 101470619 A (ANYKA (GUANGZHOU) SOFTWARE TECHNOLOGY CO., LTD.), 01 July 2009 (01.07.2009), the whole document	1-24
A	CN 1892602 A (INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES), 10 January 2007 (10.01.2007), the whole document	1-24
A	EP 0962859 A2 (SUN MICROSYSTEMS, INC.), 08 December 1999 (08.12.1999), the whole document	1-24

☐ 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
03 August 2016 (03.08.2016)	**26 August 2016 (26.08.2016)**
Name and mailing address of the ISA/CN: 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 **LI, Jia** Telephone No.: (86-10) **53311134**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/084304

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105224370 A	06 January 2016	None	
CN 101697131 A	21 April 2010	US 2012209895 A1	16 August 2012
		EP 2487585 A1	15 August 2012
		WO 2011054223 A1	12 May 2011
CN 101470619 A	01 July 2009	None	
CN 1892602 A	10 January 2007	None	
EP 0962859 A2	08 December 1999	US 6298479 B1	02 October 2001
		WO 9961970 A2	02 December 1999
		AU 4323899 A	13 December 1999
		JP 2000010792 A	14 January 2000

国际检索报告

国际申请号
PCT/CN2016/084304

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; 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））

WPI,EPODOC,CNPAT,CNKI:内核，函数地址，动态，静态，映射，对象，加载，ELF, executable and linking format, linux, unix, kernel, function address, dynamic, static, map+, object, load, ARM, x86

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
PX	CN 105224370 A (安一恒通北京科技有限公司) 2016年 1月 6日 (2016-01-06) 权利要求1-22	1-24
X	emmoblin. ". ELF可执行文件格式的理解. URL:blog.chinaunix.net/uid-20778443-id-99714.html" 20010123, 第1-7页	1-24
A	CN 101697131 A (中兴通讯股份有限公司) 2010年 4月 21日 (2010-04-21) 全文	1-24
A	CN 101470619 A (安凯广州软件技术有限公司) 2009年 7月 1日 (2009-07-01) 全文	1-24
A	CN 1892602 A (中国科学院计算技术研究所) 2007年 1月 10日 (2007-01-10) 全文	1-24
A	EP 0962859 A2 (SUN MICROSYSTEMS, INC.) 1999年 12月 8日 (1999-12-08) 全文	1-24

☐ 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
2016年 8月 3日	2016年 8月 26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 李佳 电话号码 (86-10)53311134

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/084304

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	105224370	A	2016年 1月 6日		无		
CN	101697131	A	2010年 4月 21日	US	2012209895	A1	2012年 8月 16日
				EP	2487585	A1	2012年 8月 15日
				WO	2011054223	A1	2011年 5月 12日
CN	101470619	A	2009年 7月 1日		无		
CN	1892602	A	2007年 1月 10日		无		
EP	0962859	A2	1999年 12月 8日	US	6298479	B1	2001年 10月 2日
				WO	9961970	A2	1999年 12月 2日
				AU	4323899	A	1999年 12月 13日
				JP	2000010792	A	2000年 1月 14日