

网管会公开课

2021 · 第三期



山东大学(青岛)网管会
Shandong University (Qingdao) Student Network Association



山东大学镜像站

UEFI 系统引导简介



齐划一

✉️ qi@huayi.email

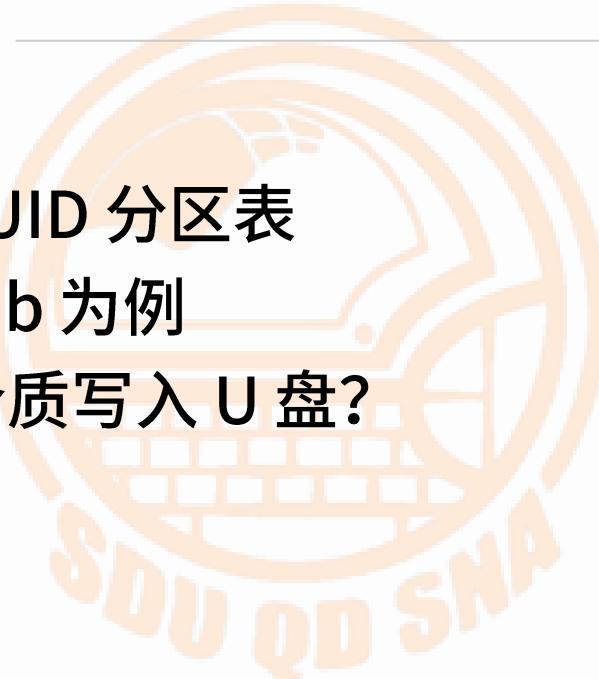
🏫 山东大学





内容提要

- UEFI 启动过程简介与 GUID 分区表
- 常见的 EFI 程序，以 grub 为例
- 如何将 Windows 安装介质写入 U 盘？
- 硬盘对拷的注意事项



1

UEFI 启动过程简介 与 GUID 分区表





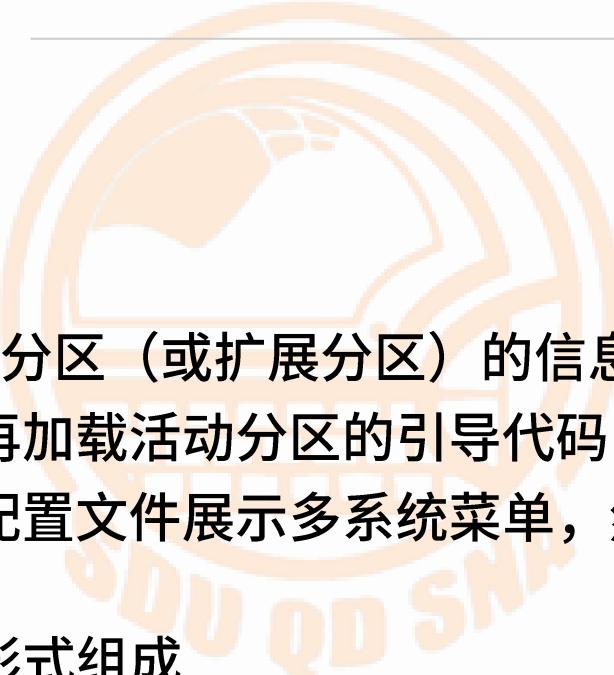
分区表

为了更好地组织硬盘



过时的 MBR 分区表和 BIOS 启动

- 只使用硬盘最开头的 512 字节
- 前 446 字节存储引导程序
- 接下来的 64 字节存储存储四个主分区（或扩展分区）的信息
- 引导程序通常会寻找活动分区，再加载活动分区的引导代码
- 活动分区的引导代码通常会根据配置文件展示多系统菜单，然后加载指定的操作系统内核
- 扩展分区由多个逻辑分区按链表形式组成





过时的 MBR 分区表和 BIOS 启动

- 支持最大 2 TB 的硬盘（假设扇区大小为 512 字节）
- 作为系统盘，仍在部分电脑中被使用的原因：
 - 电脑主板过旧，不支持 UEFI
 - 操作系统过旧，不完全支持 UEFI（例：Windows 7）
 - 结构简单，在虚拟机中便于批量部署、迁移
 - 用户不知道应该使用更先进的 GUID 分区表
- 作为数据盘，仍在部分电脑中被使用的原因：
 - 操作系统过旧，不支持 GUID 分区表（例：Windows XP）
 - 用户不知道应该使用更先进的 GUID 分区表
 - U 盘通常只有单个分区，且需要兼容多种设备



MBR + BIOS 面临的问题

- ◉ 我有多块硬盘，启动时报错找不到引导数据，怎么办？
 ㈡ 请在 BIOS 设置中手动设置第一硬盘为启动盘。
- ◉ 我是土豪，我的系统盘容量超过 2 TB 了。
 ㈡ 请额外安装一块小容量的硬盘或者 U 盘当作启动盘。
- ◉ Windows/黑苹果启动画面是 4:3 的，分辨率很低，很难看。
 ㈡ 忍着。
- ◉ 逻辑分区是链表，可靠性太低，MBR 分区表也没有额外备份。
 ㈡ 你只分一个主分区不就完了？



MBR + BIOS 面临的问题

- 多系统启动时，引导程序完全依靠“第X块硬盘第Y块分区”的方式定位不同的操作系统，太不可靠了。
- (=) 每换一次硬盘，就重新生成一次引导配置文件。
- 我想删掉 D 盘，把空余空间匀给左边的 C 盘，但是 D 盘是逻辑分区，删掉之后其空余空间依然属于扩展分区，而 C 盘是主分区，似乎无法直接调整容量？
- (=) 要么在最开始规划好容量，要么用第三方软件对分区表进行彻底修改。



MBR + BIOS 面临的问题

- ◎ 我想制作一个可启动 U 盘。
- ㈡ 既然是传统的 MBR + BIOS 方案，这个制作过程必然涉及到 MBR 引导数据、活动分区、主分区的引导记录，别想手动制作了，乖乖用各种软件吧。





GUID 分区表 (GPT)

- 在硬盘的开头和结尾均存储了分区信息，以避免分区表丢失的情况
- 取消了主分区和逻辑分区的区分，但习惯上仍然称普通分区为“主分区”
- 每个分区都有唯一的 GUID (UUID)，避免了引导程序“第X块硬盘第Y块分区”的愚蠢定位方式
- 取消了活动分区的设计，以 EFI 系统分区取代。此分区为 FAT32 文件系统，存储的 .efi 文件即为引导程序。
例如：\EFI\BOOT\BOOTX64.EFI 文件。
- 题外话：猜一猜 .efi 文件的结构与哪种文件相同?
A. Linux 的可执行文件 (ELF) B. Windows 的可执行文件 (EXE)



UEFI 启动

- 传统的 BIOS 并无能力识别分区表和文件系统，只能加载硬盘固定位置的 MBR 引导数据。甚至无法做到自动适应多硬盘启动。
- UEFI 本身能够识别 GUID 分区表、MBR 分区表和 FAT32 文件系统，会自动寻找 EFI 系统分区，并加载引导文件。若失败，则寻找所有能够识别的分区，并加载引导文件。
- 传统意义的 BIOS 早已消失，UEFI 本身具有 CSM 模块，可用来模拟传统 BIOS 启动，兼容过时硬件。
- 注：习惯上，除了严格将 BIOS 与 UEFI 进行区分、对立的语境下，BIOS 一词通常代指 UEFI。



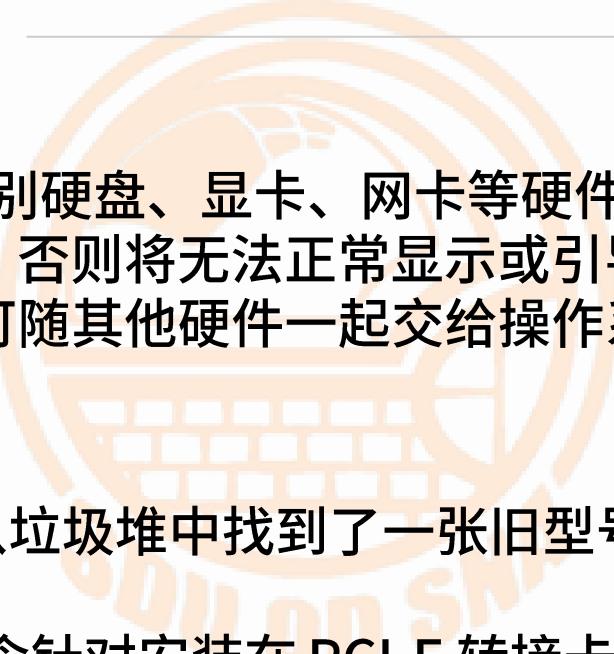
思考

- 在传统的 MBR+BIOS 启动下，系统盘往往是一个主分区，且为活动分区，主分区内同时包含引导程序和操作系统本身。在 GPT+UEFI 启动下，为什么往往使用一个 EFI 系统分区+一个主分区的方式，而不依然采用一个主分区的方式引导系统？
- 在 Linux 下，人们往往使用 dd（逐扇区复制）的方式进行硬盘对拷。假设源硬盘是 GUID 分区表，1 TB 容量，目标硬盘为 2 TB 容量，使用 dd 进行硬盘对拷，拷贝后两个硬盘依然同时存在于电脑上，不进行特殊处理。这种情况下会存在什么问题？举出两种问题。
- 你是否同意该说法：制作一个 UEFI 下的 Windows 8 启动 U 盘很简单，按 FAT32 文件系统格式化 U 盘，把 Windows 8 的 ISO 镜像内的所有文件复制到 U 盘的根目录下即可。



UEFI 驱动

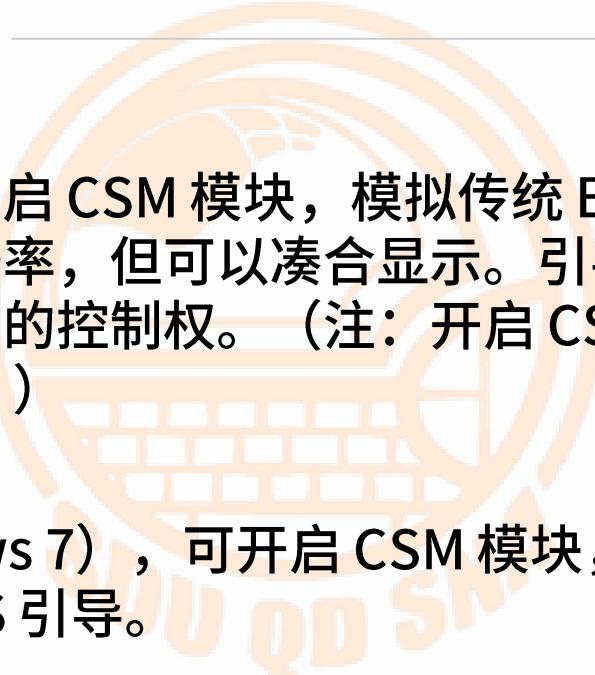
- UEFI 需要内置驱动程序以正确识别硬盘、显卡、网卡等硬件。其中，硬盘、显卡的正确驱动非常重要，否则将无法正常显示或引导系统。而网卡并非引导时的必需组件，可随其他硬件一起交给操作系统内核进行驱动。
- 不能正确驱动的例子：
 - CPU 无核显，独显价格高，从垃圾堆中找到了一张旧型号显卡（无 UEFI GOP）
 - 老主板，支持 UEFI，但不包含针对安装在 PCI-E 转接卡上的 NVME 硬盘的驱动





CSM 模块

- 针对无 UEFI GOP 的老显卡，可开启 CSM 模块，模拟传统 BIOS 的方式操作该显卡，无法支持高分辨率，但可以凑合显示。引导操作系统内核后，由操作系统接管显卡的控制权。（注：开启 CSM 模块后依然可以选择 GPT+UEFI 引导。）
- 针对过时的操作系统（如 Windows 7），可开启 CSM 模块，模拟传统 BIOS 的方式进行 MBR+BIOS 引导。
- 最佳实践：尽可能关闭 CSM 模块，除非有明确打开的理由。





思考

- ◉ 21世纪10年代，黑苹果论坛上经常会出现关于旧显卡刷入 UEFI GOP 支持的讨论贴。为什么显卡 UEFI GOP 的讨论主要集中在黑苹果？
- ◉ Windows Vista 系统早已支持 UEFI 启动，为什么 Windows 7 系统依然需要依赖 CSM，不完全支持 UEFI？是 Windows 7 对什么硬件的驱动模块存在问题？
- ◉ 假设你有一块不具备 NVME 硬盘驱动的老 UEFI 主板，可以通过什么手段将 Windows 10 系统装在这块 NVME 硬盘上，并正常引导？答出两种手段。



安全启动

- 此功能要求 CSM 必须关闭。若开启安全启动，则 .efi 文件必须具有微软或其他可信方的数字签名，UEFI 才能引导该文件。
Windows 8+ 的 bootmbr、Ubuntu 的 grub 等引导程序具有可信的数字签名。“引导区病毒”成为历史。
- 归根结底为 root of trust 问题，安全启动的开启与否并不能体现系统的安全性。
- Windows 在检测到安全启动后，会采用更严格的驱动加载策略。
- 使用 Linux 时一般应关闭安全启动，尤其是需要自行编译内核等场景。



TPM

- 可信加密模块。可安全地存储密钥，用于硬盘 BitLocker 加密等用途。Surface 电脑出厂时默认开启 TPM 并启用全盘 BitLocker 加密，让电脑变得“像 iPhone 一样安全”，即使被盗也不用担心数据泄露问题。TPM 检测到环境异常（如不同的操作系统）时可拒绝工作。
- TPM 分为独立 TPM 和集成 TPM。常见的集成 TPM 有 Intel CPU 的 Intel PTT 技术、AMD CPU 的 fTPM 技术等。Windows 11 要求 TPM 2.0 模块才能正常进行系统安装。
- 题外话：Surface 拒绝支持 Thunderbolt 3 协议，理由是该协议具有安全漏洞，攻击者可直接访问内存数据，绕过锁屏密码。你认为 Surface 这样做合理吗？



思考

- ◉ 使用 PE（例如：微 PE）引导系统通常可以用来清空忘记的 Windows 账户密码，对于基于 TPM 的 BitLocker 加密来说，也可以这样做吗？
- ◉ 你该如何权衡基于 TPM 的 BitLocker 加密的数据安全性与可用性？例如，若 TPM 模块拒绝工作，或你忘记了 Windows 账户密码，或 Windows 系统本身出现了故障，如何取回你的数据，防止数据丢失？

2

常见的 EFI 程序





常见的 EFI 程序

- EFI Shell：相当于 UEFI 下的 DOS（不完全是），可在命令行界面下浏览文件、执行其他 EFI 程序、刷写主板固件等。
- Memtest86：进行内存测试的实用程序。闭源软件。
- bootmgr：Windows 的引导程序。其引导配置文件可通过 BCDEdit 或第三方软件进行修改。
- grub：Linux 下较为常用的引导程序之一。安装 Arch Linux 时，你需要手动操作 grub-install、grub-mkconfig 命令以配置 grub。
- rEFInd：界面较为漂亮的第三方引导程序。
- ventoy：可加载 ISO 镜像，然后加载对应的引导程序。启动盘数量特别多的时候很方便。



grub

- UEFI 加载 \EFI\grub\grubx64.efi 程序
- grub 会根据配置信息，在合适的位置寻找 grub 配置文件，例如 /boot/grub/grub.cfg
- grub.cfg 中通常包含 Linux 内核的启动项，指定了内核启动参数，然后加载 initrd 和 vmlinuz，以便进行后续的 Linux 引导工作。
- grub.cfg 中还可能包含其他启动项，例如 Windows。
- 通常而言，grub.cfg 文件不是手动编写的，大部分 Linux 发行版会通过更合适的方式管理 grub.cfg 文件，这意味着不可以手动修改此文件。例如，Debian、Ubuntu 中通过 /etc/default/grub 文件指定部分参数，通过 update-grub 命令更新 grub 配置。



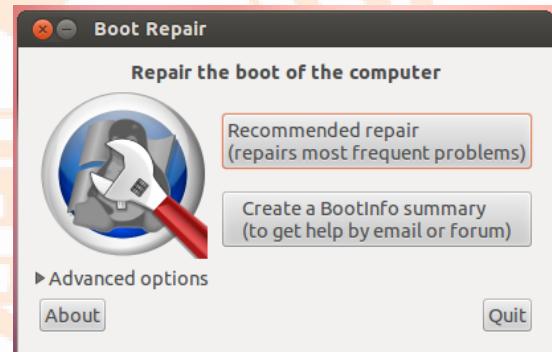
思考

- 一台电脑开机时出现 grub rescue 提示，最可能是什么原因？
- 有的 Linux 默认将 /boot 分区和系统根 / 放置在同一分区中，即作为 Linux 系统分区的一部分，你认为这样做好还是不好？举出几个优点和缺点。按引导程序和具体操作系统相分离的原则，你心目中的完美的做法应当是怎样的？
- UEFI 在没有设置对应的 EFI 变量时，只会寻找 \EFI\BOOTX64.EFI 文件。而 grub 的引导文件为 \EFI\grub\grubx64.efi。安装程序是如何做到让电脑开机时自动加载 grub 的？举出两种做法。
- 除了 grub.cfg 文件，Linux 系统下通常还有哪些文件可能是系统管理的，不能手动进行修改替换？若强行进行修改会造成什么后果？



boot-repair 工具

- <https://help.ubuntu.com/community/Boot-Repair>
- 可用于修复 Ubuntu 的引导，并且会自动检测共存的 Windows 系统
- 默认情况下会联网上传报告，需要取消此选项，否则运行极为缓慢
- 不是 Ubuntu 启动盘的一部分，需要在 Ubuntu livecd 下联网安装





NT6 引导修复

- 许多 PE（例如微 PE）自带了名为“NT6 引导修复” / “UEFI 引导修复”的工具，用来修复 Windows 引导。即使 EFI 系统分区不慎丢失，也可从容地格式化 EFI 系统分区，并通过此工具指定 Windows 的路径，补足所需的 Bootmgr 相关文件。



3

制作可启动 U 盘





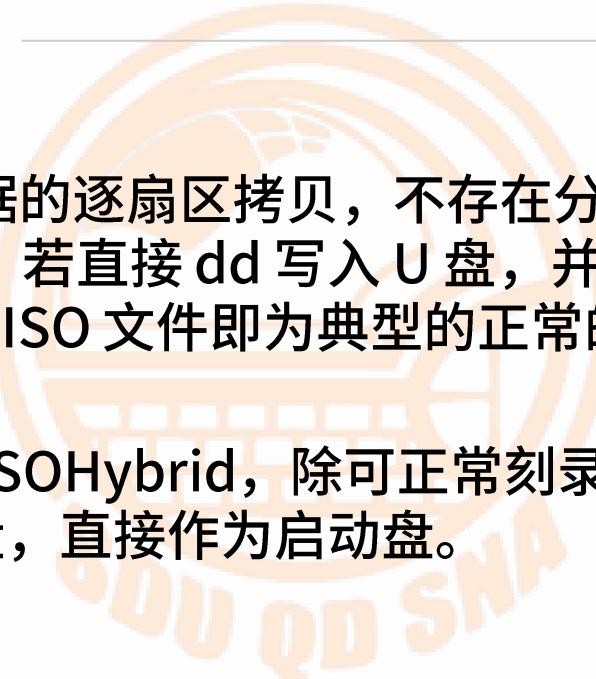
ISO 与 ISOHybrid

- ◉ ISO 文件是对光盘的逐扇区拷贝。可使用 dd 命令完成复制。
- ◉ 并非所有光盘都拥有扇区的概念。音频 CD、VCD 是基于轨道的，你无法对这些光盘制作 ISO 文件。
- ◉ 一个光盘可以同时拥有数据轨道和音频轨道，例如 1997 年的游戏资料片《红色警戒：劫后余生》光盘，同时存储了游戏的安装程序和五首 CD 音频。由于只有数据轨道具有扇区概念，若对此光盘制作 ISO 文件，则只有数据轨道的内容得以保存，而 CD 音频数据会直接丢失。
- ◉ 光盘的文件系统通常为 CDFS、UDF。



ISO 与 ISOHybrid

- 由于正常的 ISO 文件是对光盘数据的逐扇区拷贝，不存在分区表，且文件系统为 CDFS 或 UDF，若直接 dd 写入 U 盘，并不能成功作为启动盘。Windows 的 ISO 文件即为典型的正常的 ISO 文件。
- 常见 Linux 发行版的启动盘满足 ISOHybrid，除可正常刻录到光盘外，还可以直接 dd 写入 U 盘，直接作为启动盘。





制作 Windows 安装 U 盘

- 不能直接 dd / Win32DiskImager 写入 U 盘，因为不是 ISOHybrid。
- 方法一：U 盘格式化为 FAT32 文件系统，将所有文件拷贝到 U 盘根目录。缺点：FAT32 文件系统最大支持 4 GB 文件，而现在的 Windows 安装光盘的 install.wim 文件已经超过了 4 GB。
- 方法二：利用微软提供的媒体创建工具制作 Windows 安装 U 盘。由于此种方法使用高压缩率将 install.esd 文件控制在 4 GB 以内，因此可继续使用 FAT32 文件系统。缺点：需要联网，进度不可控。
- 方法三：U 盘格式化为 NTFS 文件系统，其余同方法一。缺点：主板的 UEFI 固件没有义务支持 NTFS，只有部分主板能够成功发现 U 盘内的 .efi 文件进行引导。



制作 Windows 安装 U 盘

- 方法四：利用 Rufus 工具，制作双分区方案，在较小的 FAT32 分区内使用第三方 .efi 引导程序（含 NTFS 驱动），负责寻找同 U 盘的 NTFS 分区，并加载该分区的安装程序。缺点：该程序没有微软的数字签名，开启安全启动功能的 UEFI 会拒绝执行此程序，需手动关闭安全启动。
- 方法五：制作微 PE 工具箱的启动 U 盘，并通过微 PE 内包含的 Windows 安装器完成系统安装。缺点：缺乏安装向导，需要用户对 PE 的操作、GUID 分区表、UEFI 启动具有一定的了解。
- 方法六：使用 ventoy 加载 Windows ISO。缺点：需手动关闭安全启动。



制作 Windows 安装 U 盘

- ◎ 总结：看似这么简单的需求，居然没有银弹。每种方法都有弊端。





思考

- （本题使用 Windows 的单位，即 $1\text{ MB} = 1024\text{ KB} = 1048576\text{ B}$ 。）一张 700 MB 的光盘既可以选择写入 700 MB 的数据文件，也可以写入 80 分钟的 CD 音频。计算一下空间占用：CD 音频的比特率为 1411.2 Kbps，因此每秒钟所占用的空间为 $1411.2\text{ Kbits} = 172.265625\text{ KB}$ （说除以 8 的，动动脑子），即约为 0.16823 MB，因此 80 分钟的 CD 音频应当占用大约 807.50 MB 空间。这与光盘的 700 MB 容量似乎有矛盾。查阅资料，找到 700 MB 光盘能够顺利放下约 800 MB 音频数据的原因。

4

硬盘对拷





硬盘对拷

- 当前为 2021 年，许多电脑出厂的固态硬盘容量有限，多为 256 GB、512 GB。随着固态硬盘制作工艺提升，售价降低，1 TB、2 TB 的固态硬盘越来越流行。保留原有系统并更换固态硬盘是一个热门需求。
- 将新固态硬盘装入电脑，将旧固态硬盘放入移动硬盘盒中，也接入电脑。接着，可使用 Linux 启动盘启动，并通过 dd 完成硬盘对拷；也可使用微 PE 启动，通过附带的 DiskGenius 软件完成硬盘对拷。
- 前文的思考题提到，这样的对拷完成后，新旧硬盘的分区 GUID (UUID) 完全相同。而这会导致混乱。因此，最佳做法是，在硬盘对拷完成后，立即关闭电脑，并移除旧硬盘。千万不要同时连接新旧硬盘并启动系统。



硬盘对拷

- ◎ 千万不要同时连接新旧硬盘并启动系统。否则，由于两个硬盘的分区 GUID (UUID) 相同，Windows 启动时的盘符挂载关系会被打乱，会导致 Windows 继续将旧硬盘的系统盘作为 C 盘，将新硬盘的系统盘作为其他盘符挂载。此时，即使移除了旧硬盘，单独使用新硬盘启动，Windows 的盘符挂载关系也不会恢复，此时系统内不存在 C 盘，无法正常进入系统，只能人工修复。
- ◎ 修复方法：进入微 PE，打开注册表编辑器，远程挂载注册表 HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices（不是打开 PE 本身的注册表），将该键下的键值全部清空。提示：挂载 \Windows\System32\config\SYSTEM 文件。



Thanks!

Any *questions* ?



齐划一

qi@huayi.email

山东大学