计算机类发明技术交底书提纲

### 技术交底书是代理人撰写专利申请文件的依据，其要针对某一发明创造（以下简称发明）主题，说清楚别人是怎么做的？别人做的有什么缺陷？我要做什么？我是怎么做的？我做的关键点在哪里？我做的有哪些优点？

1、本发明的名称

2、背景技术的方案

3、背景技术的缺陷

4、本发明的目的

5、本发明的实施方案

6、本发明的关键点

7、本发明的效果

8、背景技术和本发明的附图

一、本发明的名称

此部分简要揭示发明主题，需清楚说明本发明的产品名称和/或方法名称，不要含有人名、单位名、商标、代号和型号等非技术术语。

一种以劫持方式进行视频解密的方法及装置

二、背景技术的方案

此部分简要说明别人是怎么做的？需先简要介绍本发明涉及的技术和/或产品的性质和用途等；接下来简要介绍1到2项与本发明最接近的背景技术，即与本发明有相同目的或相同技术手段或相同用途的产品或方法，最好不是综述。

背景技术既可以是文献中的技术，也可以是常识或现有产品，是文献时需详细说明背景技术的文献出处，如专利文献号，或期刊名称、卷号、期号和页码，或书籍名称、作者、出版者、版次和页码。介绍背景技术时，应当重点说明背景技术方案的功能和实现过程。

数字视频内容通常通过数字版权管理（DRM）技术进行保护，以防止未经授权的访问和复制。这些DRM系统通常在终端设备上运行，以解密和播放受保护的视频内容。然而，一些情况下，用户可能需要对视频内容进行合法的解密，以便进行备份、格式转换或其他合法用途。

已有的数字视频解密方法通常涉及破解DRM系统，这可能涉及法律风险和侵犯知识产权的问题。因此，有必要提供一种安全、合法且有效的方法，以劫持方式进行视频解密，以维护数字版权和用户合法权益的平衡。

1. 背景技术的缺陷

此部分简要说明别人做的有什么缺陷？需要客观说明各背景技术的方法或产品在工艺或性能上的不足。但最好能结合背景技术的技术方案，介绍为什么会存在这样的缺陷。

不便的用户体验：DRM系统通常需要用户进行授权、注册或登录，以获取解密所需的密钥或许可证。这可能会导致用户体验不佳，降低了用户观看视频内容的便利性。

限制性：DRM系统通常限制了用户对数字视频内容的使用，例如，可能限制了视频内容的播放设备、转码、备份等操作。这限制了用户对数字视频的自由使用。

漏洞和攻击：DRM系统存在被攻击和破解的风险。黑客和逆向工程师可能会试图破解DRM系统，以获取解密密钥或绕过保护措施，这可能导致版权侵权和非法分发。

不同DRM系统的不兼容性：不同内容提供商可能使用不同的DRM系统，这导致了DRM系统之间的不兼容性。用户可能需要安装多个DRM解密器，以便在不同平台上观看受保护的视频内容，这增加了用户的不便。

四、本发明的目的

### 此部分简要说明我要做什么？需要简要说明本发明要克服的缺陷，或要解决的问题，或要达到的目的，应当结合上述“背景技术的缺陷”进行说明。

本发明的目的就是提出一种方法不需要获取解密key直接读取还原经过drm加密的视频数据。本发明在不需要获取解密key ，直接读取还原经过drm加密的视频数据，以实现对数字视频内容的合法解密。

五、本发明的方案

此部分详细说明我是怎么做的？需要详细说明本发明的总体技术方案，本部分内容是技术交底材料的核心部分，也是内容最多的部分，此部分的内容需要重点突出展现本发明的技术原理、实现过程、技术措施、技术改进点等，如果技术改进点在于系统结构（或硬件结构）的变化，则最好给出系统硬件结构图，并且结合系统结构图说明系统的工作原理和工作过程，如果技术改进点还包括数据处理过程或步骤，则最好还能给出类似软件设计中常用的时序图（流程图）和功能框图，特别对于某些设计算法改进型的技术方案，还必须给出改进后的算法计算式。

图1 是一种直接读取还原经过苹果T2芯片加密的磁盘数据功能。该方案包括：

S10：快速**检测Mac设备是否含有T2 芯片方法**

通过命令system\_profiler获取系统设备属性，根据属性选项的SpiBridgeDataType值中是否包含Apple T2字符来确定该设备已经包含了T2芯片

**S20：加载我们开发的内核扩展驱动**

在S10模块已经确定该设备拥有T2芯片后， 开始准备加载我们准备的内核驱动扩展kext，首先对驱动文件权限进行修改，将其权限修改为可执行权限，并将其加入root:wheel群组中

驱动文件权限修改完毕后，通过调用LoadKext管理函数来将我们驱动加载到内核中

S30：执行替换加密磁盘的策略例程函数流程

1.驱动在加载初始化时，我们的驱动功能开始遍历IO设备，找到提供IOMedia服务的设备对象，这些设备即为iMac下的磁盘存储设备，进一步获取该设备的IOBSDName属性,并判断该属性值是否为“disk0”，

如果是disk0则该磁盘为我们要找到的主硬盘， 而不是外接的移动硬盘，因为iMac默认只会对自带的主硬盘用T2芯片进行加密

2.找到主硬盘设备对象后，我们需要获取 该硬盘的 IOBSD核心ID号（IOBSDMajorKey），以及数据块大小，如果块大小为0字节，获取则直接指定块大小为4096字节，因为APFS分区的数据块大小默认4096字节

3.通过上一步获取的设备IOSBD核心ID，通过驱动内核函数，移除掉该设备对象的块设备切换表，该表中记录了块设备会被调用到的打开、关闭、策略例程、获取大小、获取类型操作对应的处理函数

4.在上一步移除原有的块设备表之后，通过复制创建新的块设备转换表，在原有表基础上只修改替换策略例程函数，将其中策略例程函数更换为我们自己的策略例程函数，并通过内核函数，将新的块设备转换表添加到主硬盘设备对象中，此时在读写主硬盘设备文件时将会进入我们自定义的策略例程函数中

S40 构造配合驱动的主程序端

该主程序端负责通知驱动程序读取加密磁盘中任意指定分区内的数据块，以及负责再经过驱动程序处理后，读取解密后的磁盘数据的任务

S50主程序端构造触发自定义策略例程函数的**自定义唯一文件**

在主磁盘的指定分区中创建一个随机的32位长度GUID命名的文件名，这样可以避免和其他正常已存在的文件名称相同，导致冲突，该分区为将要扫描或者读取的分区，主磁盘中可能存在多个分区，将文件大小设定为以后一次性从加密磁盘中读取指定块大小，这里我们设定为0x10000个字节来提高读取效率

S60 主程序端通知驱动记录**指定读取数据的磁盘物理偏移地址**

1. 遍历本地已经加载的驱动，并通过驱动类名称匹配找到是我们自己创建的驱动程序，创建并连接驱动服务，准备与驱动程序进行交互通信
2. 通知驱动记录将要读取的磁盘分区下的指定数据块的磁盘物理位置偏移地址，该地址是由 要读取的数据块ID （BlockID）乘以 BlockSize计算得出，将位置发送给驱动，驱动程序触发记录将要 读取的磁盘物理位置偏移地址的流程，记录保存物理位置偏移地址

S70 主程序读取创建的自定义唯一文件 触发进入自定义策略例程函数

1.主程序打开之前创建的GUID 32位长度的文件，并设置文件偏移，从文件偏移0开始读取，读取0x10000字节数据

2.在我们主程序读操作时，会自动触发进入我们驱动之前替换的自定义策略例程函数中

S80 自定义策略例程函数执行替换 指定想要读取的磁盘物理地址

1.当系统中有在读写主硬盘设备文件时，通过系统内核回调进入我们自定义的例程函数中，我们首先判断 系统读写缓冲区记录中是否存在数据，存在则从缓冲区中读取文件系统相关记录，从记录中获取与缓冲区相关的vnode节点名称

2.该名称为系统中读取主硬盘中文件时所打开的文件名称，我们进一步判断该vnode节点名称是否为 我们之前主程序端 创建的以32位长度的GUID为文件名的名称，如果是，则进入后续修改BlockID位置的流程，如果不是则直接调用系统原有的策略例程函数dkstrategy，而不影响其他程序的正常读写功能

3.修改物理偏移地址，首先我们要在缓冲区的记录数据buf结构中找到 存放将要读取的32位 GUID命名的自定义文件数据块在磁盘上的物理偏移地址， 首先获取该文件在磁盘上的数据块号BlockID， 通过数据块号与之前获取的块大小BlockSize相乘得到具体磁盘物理偏移地址，

然后进一步在缓冲区的记录数据buf中搜索磁盘偏移地址，找到存放该偏移地址的位置。接下来我们在该位置设置替换为我们主程序指定扫描读取的数据块对应的磁盘物理位置偏移地址，**并通过**设置与缓冲区关联的物理块号（**setblno**）为我们指定要读取的数据块号BlockId，(磁盘物理位置偏移地址除以之前获取的块大小，得出对应指定的BlockId)，修改完毕后，我们自定义的策略例程函数再调用真正的策略例程函数，将处理流程交给真正的策略例程函数执行，后续系统会和T2芯片交互返回解密数据块

S90 主程序接收读取解密后的指定磁盘位置数据

在主程序读取操作完毕后，主程序读取出来的0x10000字节数据，并非我们前面创建的文件本身的数据，而是我们经过驱动修改指定为要扫描读取数据块的数据

此过程包含了 主程序和驱动的交互通信过程，完成读取加密磁盘分区中任意位置已经解密的数据块内容

六、本发明的关键点

此部分的作用是让专利代理人能更清楚地认识本发明技术方案的发明点或“闪光点”，便于专利代理人在撰写专利申请文件时把握正确的方向。

本发明在通过编写内核扩展驱动，重新绑定指定主磁盘的块设备转换表，在原有表基础上替换策略例程函数**，并通过主程序模拟创建一个自定义唯一文件，在自定义策略例程函数中搜索存放将要读取 该文件的磁盘物理偏移地址并替换为我们指定扫描读取的物理偏移地址，并通过**设置与缓冲区关联的物理块号为我们指定要读取的数据块号来达到替换效果，替换后主程序**指定读取位置，并模拟读取自定义文件触发读取磁盘指定位置的数据**

七、本发明的效果

### 此部分详细说明我做的有哪些优点？需要详细阐述本发明所达到的效果和优点。可以用产量、品质、收率产率、质量、精度、效率提高，能耗、原材料、工序的节省，加工、操作、控制、使用的简便，有利于环保、降低劳动强度，出现有用性能等的数据说明。最好与背景技术比较，用实验数据来说明发明效果；也可以从理论推导或特点分析来说明发明效果。当采用实验数据时，应给出必要的试验条件和方法。

### 计算机领域发明应说明其带来的突出效果，例如数据安全、资源节省等。例如，计算产品发明应说明与现有产品相比所具有的优点，如在数据处理速度、准确度、制造成本等方面的优点。

采用本发明所述直接读取还原经过苹果T2芯片加密的磁盘数据方法，针对T2芯片保护的磁盘，不需要解密key，不需要关闭SIP（系统完整性保护），就能直接读取加密磁盘上任意指定的解密后的数据块，用来做数据恢复扫描或者数字取证，支持最新macbook、mac mini、iMac等设备

八、背景技术和本发明的附图

此部分是上述各部分的辅助部分，需要清晰给出背景技术和本发明的工艺流程图和产品结构图等及其说明。此部分可有可无，可以是一幅，也可以是多幅。工艺流程图可以在框图内说明各工艺步骤名称，产品结构图可以将各部件用引出线通过阿拉伯数字统一标号。剖面图或局部放大图要单独给出图号。附图说明需简略说明各附图的名称以及各标记的含义。

计算机技术领域的附图主要包括系统结构图、数据流程图和功能框图等。



图1