

# 保密协议

(密级: confidential (划掉))

- 1、绝对禁止以任何方式将解密后的“大学标准学术垃圾”中的任何文件传到网上,包括但不限于百度网盘、Dropbox、Google drive 等个人网络存储,或是 QQ、Tim、Skype 等即时聊天软件。可以上传经过 Veracrypt 高强度加密的文档,但是密码长度需要大于等于 18 位,且不能是任何网络上注册账号对应的密码。
- 2、禁止使用具有自动备份或自动保存文档功能的软件浏览原文,包括但不限于 word、wps、neat office 等,可以使用记事本或写字板浏览原文。禁止在联网的电脑上浏览原文。浏览原文时请先断开网络连接,并关闭 360 安全卫士、360 杀毒、金山毒霸、腾讯管家、游戏修改器、盗版游戏等流氓公司的软件,以及其他无关软件,推荐使用虚拟机。输入密码或浏览原文前,必须确保目视范围内没有监控摄像头和可疑人员。
- 3、禁止将解密后的原文复制到加密容器以外的地方,防止留下缓存。如果因为操作失误导致硬盘上出现过解密后的原文,请立刻删除,并使用命令提示符对物理磁盘下的所有逻辑分区运行“cipher /w:盘符”指令。例如在 D 盘存放过原文,则运行“cipher /w:D”。也可以使用其他方式清除痕迹,但是不要使用国产软件。
- 4、不能以任何方式直接复制“大学标准学术垃圾”中的内容。如果想要和其他人分享文中的内容请用自己的话转述,并且不要向其他人声明内容来源于零分作文。不要让与本文无关或相关性较少的人通过“大学标准学术垃圾”知道作者和其他密钥持有人的黑历史或非主流想法。
- 5、如果密钥持有人或作者之间存在利益纠纷,不得将“大学标准学术垃圾”中的任何内容作为筹码进行谈判。作者在世时,密钥持有人应当绝口不提已经获得“大学标准学术垃圾”授权。如果作者意外亡故,密钥持有人需面见作者父母告知密钥,并联合决定是否公开以及公开的范围。
- 6、零分作文不受著作权法保护,但是协议对作者和密钥持有人均有现实约束力。如果其中一方故意违反协议并导致重大泄密事故,则该协议作废。分级加密准则和操作流程在附件中已经详细描述。输入密码便默认你会遵守上述协议。

签名区:

附件 1:

## 分级加密准则（密级：confidential **（划掉）**）

### 一级机密：

加密方式：未知。

加密内容：未知。

泄密后果：需立刻去死，并确保死的彻底，以避免进入无间地狱。

### 二级机密：

加密方式：在三级机密的基础上，考虑电磁辐射泄露、内存离线读取、毫米波探测、红外成像这样的旁路攻击，需要安全的环境以确保上述攻击无效。防范心理学层面的攻击，包括但不限于权威人格、威逼利诱、见色起意。多重加密和 25 位以上的密码，并在密码中引入数学推导，确保在不清醒时或紧张时无法打开加密文件。每次操作二级机密要检查计算机是否被安装监听设备。此外，每次操作二级机密过后，需要对内存进行全覆盖写入方可关机，如果有意外缓存的情况，立刻对硬盘进行 2 次及以上随机数写入与擦除。

加密内容：小学标准零分作文，重大且超前但不适合公开的理念、发现或发明等。

泄密后果：放弃身份和熟悉的一切，取出所有现金，变更身份，隐姓埋名，远走他乡。

### 三级机密：

加密方式：在未分级加密的基础上，按照软件使用规范利用 Veracrypt 或 Truecrypt 高强度开源加密工具对文件进行加密。不定期检查计算机是否被安装监听设备，不定期检查环境安全性，并注意防范视觉黑客的攻击。在操作三级机密的过程中，应将计算机与网络的连接断开并彻底关闭无关软件。所有三级机密的加密文件不得以解密后的状态存在于内存以外的任何空间。

加密内容：大部分标准零分作文，secret 级别的项目资料等。

泄密后果：近 5 年左右的一切非知识性积累全部归零，人际关系完全改写。

### 未分级加密（四级）：

加密方式：在五级的基础上，使用压缩包加密或文档加密（仅限 office2003 以后），并设定 8 位以上的密码。

加密内容：confidential 级别的项目资料，姿势奇怪的裸照，重大黑历史等。

泄密后果：造成重大不适和困扰，需要花费较大的代价以弥补损失。

### 未分级加密（五级）：

加密方式：明文存放在磁盘中，不在未加密情况下通过网络传输。

加密内容：账号密码，一般非公开项目资料，普通黑历史等。

泄密后果：不良后果可控。

附件 2:

## 加密软件操作流程（密级：internal（划掉））

### 加密原理：

Veracrypt 开源加密软件的主要加密算法包括 AES, twofish 等，这些算法求解的时间复杂度为  $O(2^n)$ ，理论上不可破解。以 AES256 为例，使用一台 8 核且具备 AES 扩展指令集的电脑进行破解，需要经过四百万亿年的时间，并且，尚未有证据证明量子计算机可以解决 NPC 问题。换言之，加密文件在不知晓密钥的情况下，不具备打开的可能性。

输入的密钥被存放于 RAM 中，用于对文件进行加解密。根据局部性原理，文件会依照应用程序的需求读取到 RAM 或写回到硬盘，对于较大的文件（例如 A 片），通常不会一次性将全部内容读取至 RAM，但是对于较小的文本文件，则可能一次性全部读取至 RAM。原则上讲，只要密钥和源文件只存在于 RAM 中，就是相对安全的。

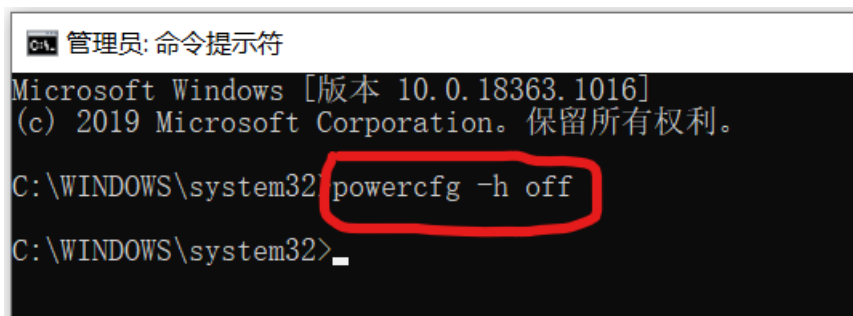
但是，加密不能保证旁路攻击的无效性，也不能保证不留下任何缓存。使用键盘记录器、屏幕录制、内存攻击、电磁辐射监测等手段都可以获得密钥或源文件内容。根据三级机密加密准则，不过多考虑旁路攻击，重点考虑缓存和流氓软件导致的数据泄露。Word 和 WPS 等现代办公软件，具有自动保存已修改文档的功能，会留下文本缓存；Windows 具有保存近期文件索引的功能、休眠功能、分页文件和内存故障转储，在特定情况下会将 RAM 中的数据写入到硬盘，这里面可能会包含密钥或被加密的原文件，大大降低了解密成本。

为了防范可能的数据泄露，请严格按照下列步骤操作。

### 准备工作：

（准备工作只需要做一次；变更设置或重装系统后，需要重新进行准备工作）

- 1、以管理员身份运行命令提示符，输入“powercfg -h off”命令禁用休眠（顺便能给电脑省出 1GB 以上空间）：



```
管理员: 命令提示符
Microsoft Windows [版本 10.0.18363.1016]
(c) 2019 Microsoft Corporation。保留所有权利。

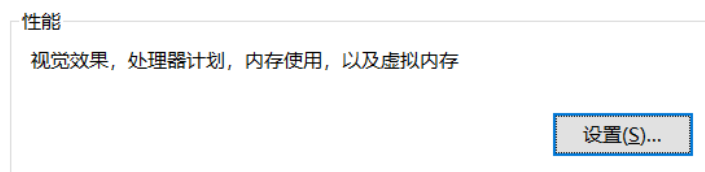
C:\WINDOWS\system32 powercfg -h off
C:\WINDOWS\system32>
```

2、右键单击“此电脑”，在“属性”中找到“高级系统设置”，如下图所示：

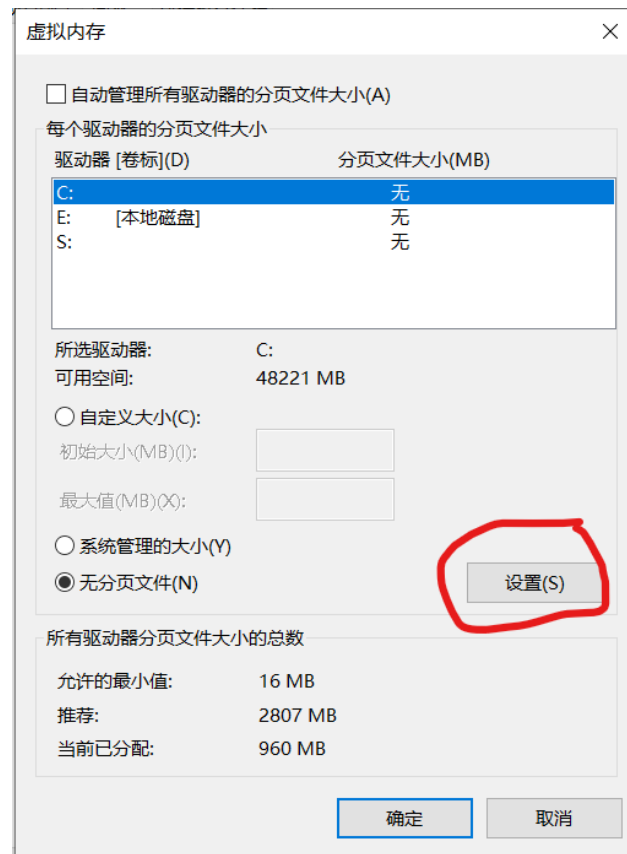


3、打开虚拟内存设置：

要进行大多数更改，你必须作为管理员登录。



- 4、更改虚拟内存，按照下图所示的方式，将所有逻辑磁盘的分页文件全部取消，系统会提出警告，请忽略这个警告（如果由于内存过小而在玩 3A 大作，使用 adobe 软件时出现问题，请重新开启分页文件，可以选择“自动管理所有驱动器的分页文件大小”）：



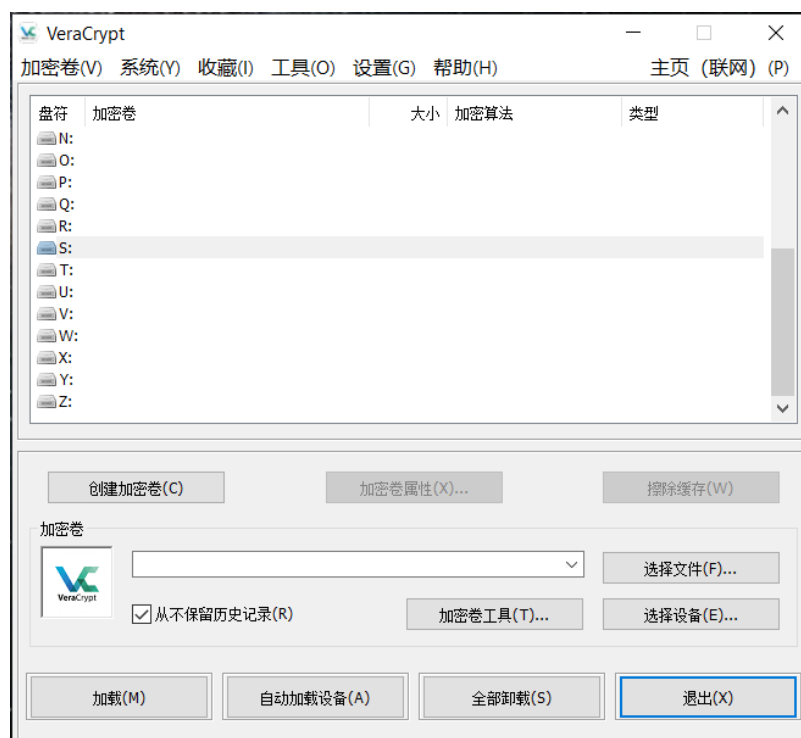
- 5、按照要求重启电脑，将虚拟内存关闭。注意保存已打开的文件，防止数据丢失。
- 6、关闭内存转储，防止系统崩溃时自动记录内存信息（这些信息对于没有 CS 基础的人来说，不会对解决系统问题有帮助，但是微软还是记录了下来），关闭内存转储的选项在“高级系统设置”中：



7、在调试信息一栏中，选择“无”：

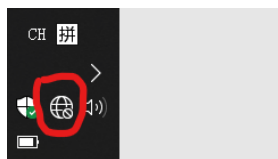


8、安装 Veracrypt 高强度加密软件（也可以不安装，直接使用），界面如下图所示：

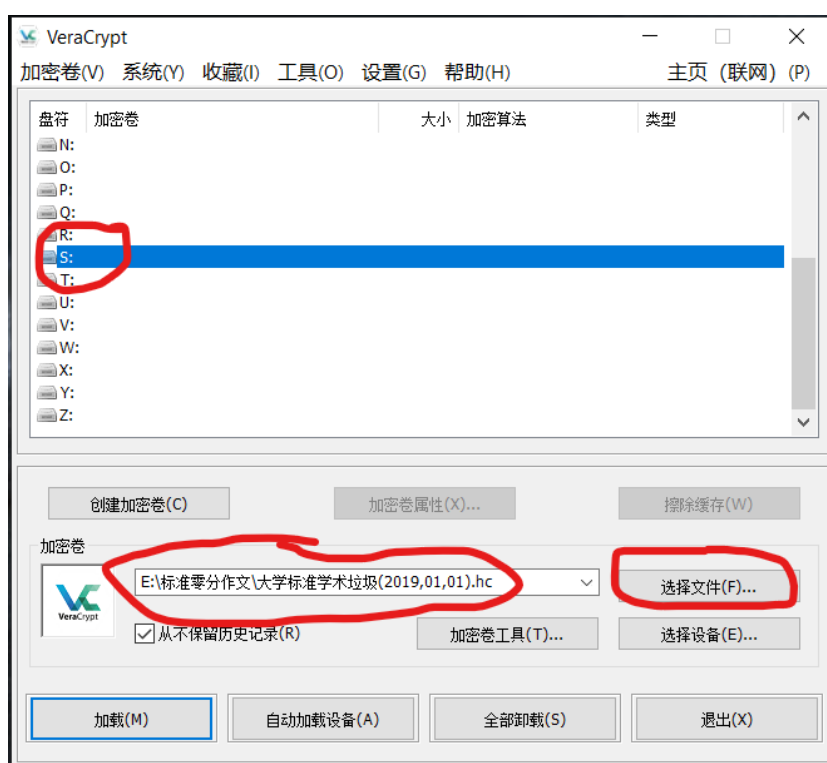


## 打开加密文件：

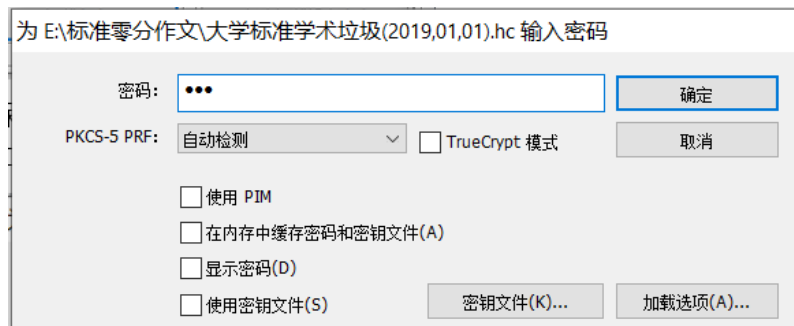
- 1、确定网络处于断开状态，如下图所示：



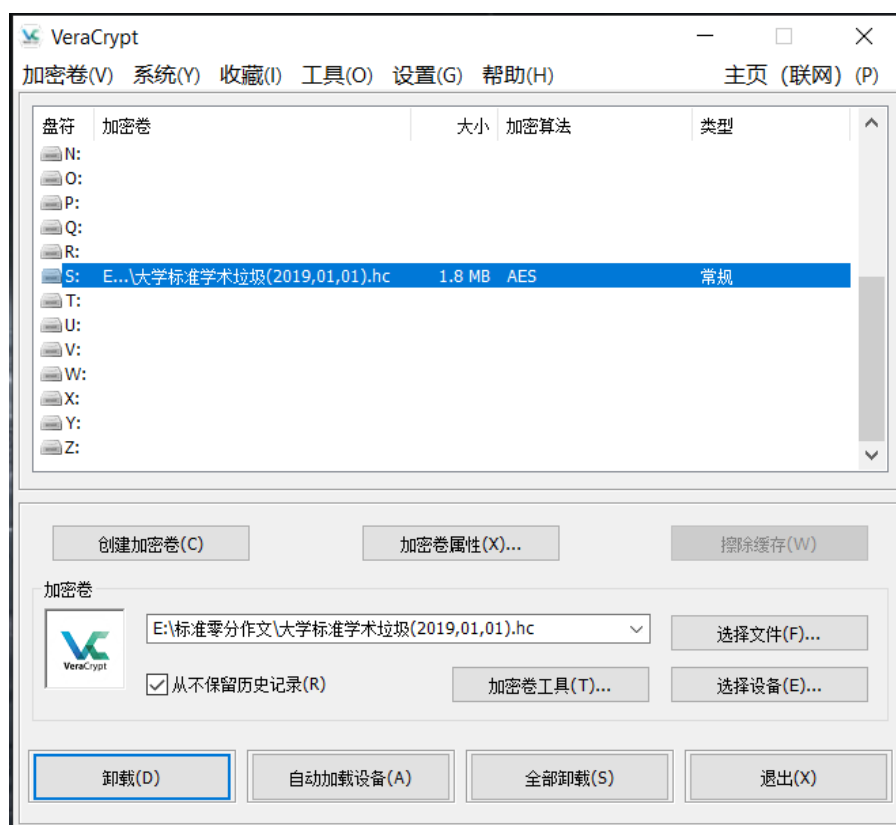
- 2、关闭所有 360 系列软件（流氓起家，本性难移）、百度系列软件（假药致富，声名远扬）、腾讯系列软件（抄袭能手，垄断寡头），以及其他不相关的软件。
- 3、打开 Veracrypt 软件，随便选择一个要挂载加密卷的盘符，此处以 S 盘为例，点击选择文件按钮，选择要打开的加密文件，这里以“大学标准学术垃圾”为例：



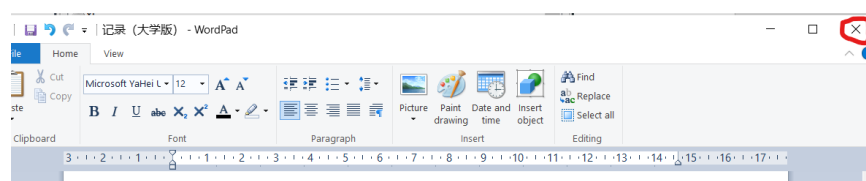
- 4、检查环境安全性，确保目视范围内没有监控摄像头和无关人员，输入密码时应当遮挡键盘，最好背对白墙以减少环境复杂度。请再次确保已经做好准备工作，并且不违反保密协议，然后点击“加载”，在对话框中输入密码，如下图所示：



- 5、点击确定，非常恭喜，你已经可以查看所有原文件了，并且具备了对作者和某些人实施无条件降维打击和极限施压的能力，但是，请不要这样做。另外，不要用 word 或 WPS 打开这些文件，请使用记事本或写字板打开。作者和密钥持有人依据保密协议保留对恶意泄密进行惩治的权利。



- 6、如果在阅读过程中感觉到不适，请立刻点击文档右上角的关闭按钮。部分内容确实不寻常，和正常思维相差极大，如下图所示：（建议用“ctrl + F”快捷键检索感兴趣的内容）



- 7、退出时，请关闭所有已打开的零分作文、其他文件和文件夹，然后点击卸载按钮，如果提示还有文件占用，在确保已经关闭的情况下可以强制卸载。（所以，不要一边开着流氓软件，一边看零分作文）





附件 3:

**拟定候选人及风险考量（密级：confidential（划掉））**

1、杨欣程：

合作时间最长，见证我大学期间 2/3 以上重大时刻，包括但不限于集创赛、大二上的艰苦时期、萌生杯；直接参与我 1/2 以上的项目和重要事件，对我的了解远超其他同学；零分作文中有大量和他相关的事迹，本人亲历过部分三级机密加密标准中记录的黑历史。但是他使用电脑的经验不丰富，可能会误操作；不确定是否接受泄密成本。

2、刘悦多：

将来会和他进行密切合作，曾协助我集创赛并取得国一；具有强于我的学习能力以及接受能力；由于杨世恒坐镇，未来不太可能存在利益冲突；对我了解较多，主要是电子设计和阴间操作方面。但是将来长期与他合作，提前知晓零分作文的内容将为我们后续的合作引入不确定因素，而且对杨欣程很不公平；不确定是否接受泄密成本。

3、陈宣霖：

预期将来会很少联系，也不太可能存在利益冲突；曾是我团队成员，经常划水，很少认真研究电路；曾一同去美国游玩，间接了解过我的事迹，也短暂接触过高考标准零分作文，有心理准备。但是没有很强的利益关联，不知是否会遵守协议；不确定是否接受泄密成本。

4、孙天一：

曾是嵌入式智能互联大赛的队友，具有不愿公开的黑历史，不太可能泄露；间接了解过三级机密“高考标准零分作文”中的事迹，不过并不完整；将在本校读研，未来可能存在合作关系。但是集创赛曾将她水掉，后续没有合作；不确定是否接受泄密成本。

5、黎洋：

曾在 IC2、魔集课中合作过，大三下学期和大四上学期经常吃饭，是我和刘悦多黑的对象，其典故包括但不限于儿童肉棒、儿童鸡皮，了解很少部分三级机密的事迹。但是泄露三级机密内容对其影响不大；不确定是否接受泄密成本。

风险考量：

零分作文系列是留给自己以及遥远未来的一份礼物，也是在时间的洪流中超越生死的伟大尝试。这一系列作品细节详实，感情真切，内容丰富，近乎完美的记录了我人生中的重要轨迹，已经超过 20 万字，在分级加密标准中位列三级及以上，注定完全不适合公开。

小学标准零分作文尚未完成（主要受心理承受能力限制），未来准备将密钥拆分后再转让给不同人。中考和高考零分作文后继有人，然而当初过于相信他们的自觉，导致实际曾被降为五级，索性暂未发现被公开的迹象，并且已经进行了纠正。大学标准学术垃圾的授权会吸取先前的教训，增加泄密成本，考虑使用实拍的裸照，以确保成员遵守保密协议。

活到现在纯属运气使然，活成现在的样子更是机缘巧合。今年已有 2 人在我眼前死去，1 人在听闻中死去，数不清的人死于瘟疫。博士生的死亡不能算作小概率事件，必须予以考虑。在认真活下去的同时，也应当留点什么给我父母，我在乎的人和其他在乎我的人。当意外发生时，零分作文是我在思维层面唯一能留下来的东西，也是唯一能够了解我真实人生的资料。授权人数越多，留存下来的可能性越大，中考和高考零分作文授权便基于此。

但是，授权零分作文面临泄密的问题，会带来非常严重的后果，人设崩塌、人际关系改写、被迫退学、返回老家甚至逃离人类社会。未来数据挖掘将更容易，存在被恶意竞争对手针对的可能。因此，本次决定只授权 1 人且不再增加授权人数，而非像先前一样有 8 人。另外，适当增加泄密的成本，防止为了方便或未来因为利益纠纷而故意违反保密协议。