


中国科学院大学
University of Chinese Academy of Sciences

对话：计算机考研复试精准定位0day思维

李敬
Li Jing

2021年2月7日

庚子年 腊月廿五

江苏 · 南通平潮

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

$ whoami

- 我叫李敬（@lix3on）
- 扬州大学2019届软件工程(NIIT)本科毕业生
- 现为2020级中国科学院信息工程研究所 / 中国科学院大学网络空间安全学院，硕博连读研究生，师从侯锐教授
- 所在科室：信息安全国家重点实验室
- 研究方向：智能芯片安全、体系结构安全
- lixeon.com
- lixeon.lij@gmail.com

Contents

Napoleon Crossing the Alps *

* https://en.wikipedia.org/wiki/Napoleon_Crossing_the_Alps

以信工所为例（2020）

今年信工所情况：

推免鸽了近60人（各种原因）

最低分265分录取,最高分402分录取

300分以下近30人

某280分大龄女录取

290-310分复试被刷占高比例（要转换表达）

某384分大佬刚六室被刷（最终去向武大）

某370+大佬复试前跳车（最终去向上科大）

调剂13个，355网络中心难民录取

调剂某本科北大330+大佬被刷

还补录了一个，天选之子

诚实诚心是录取关键

慎做考研渣男渣女

部门名称	指标数	报考数	平均分(±1)	预选比例估计	实际跳车	录取	招调剂	备注	填写信息且录取比
信安国重	49	53	334.8113	51.761194	1	44	6	录取中含1士兵计划	66.03%
第二研究室	23	40	310.3636	33.4925373		23	1	录取中含1少干计划	27.50%
第三研究室	16	22	324.5263	19.7910448		13	3+1(补录)		36.36%
第四研究室	30	41	307.1794	44.1492537		30	0		48.78%
第五研究室	28	30	309.3333	31.9701493		26	3	录取中含1少干计划	56.67%
第六研究室	13	18	323.4210	22.8358209		14	0	录取中含1士兵计划	55.56%
合计	159	204				150	13	4	

流程相关准备

- 线下流程：心理测试、【基础笔试/上机（算法 or CTF）】、面试
- 线上流程：【上机（算法 or CTF）】、面试
- 面试含英语面试、技术面试、综合面试
- 关注官网通知
  - http://www.iie.cas.cn/xsjy2020/zxtz2020/
- 可以带着看过往历年复试经验帖
  - 如有笔试，题肯定或多或少都见过，且可开放性回答
- 现在是时候详细了解信工所各方面情况了
  - https://github.com/lixeon/iiecas-kaoyan-bo-docs
- **线上线下基本区别不大**
- **重点关注面试环节**

进度管理

- **信工所复试时间一般较晚**
- 可适当跳车，留给后面的乘客
- 至少要整理好本科期间做过的相关工作
- 然后年前应当出炉第一份简历
  - 复试前根据需要修改
  - 一般都会针对格式、内容改2-3次
- 复试前最好联系老师
  - 老师有回复（进一步对话）
  - 老师无回复（再润色）
- 复试前几周准备好英文介绍
- 复试时把握对话时间和节奏
- 复试后联系老师（不论之前是否有联系过）

坚持才能抄底

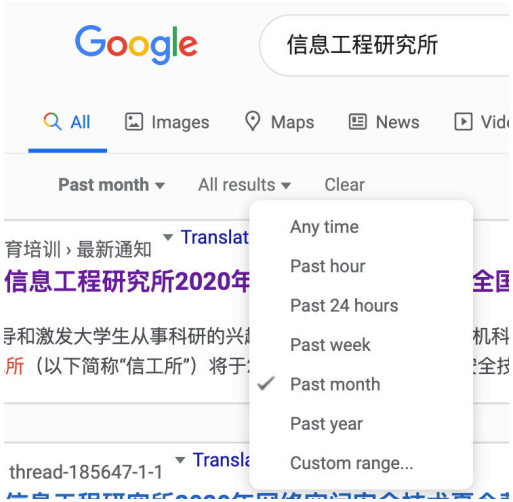
- 兵临城下，入关在此一举
- **复试没有真题**
- **复试不需要真题**
- 复试真题思维相对低维，要对话思维
- **复试策略核心概括为四控三管一协调**
- 过线就可以稳，稀里糊涂就抄底了
- 咬定青山不放松

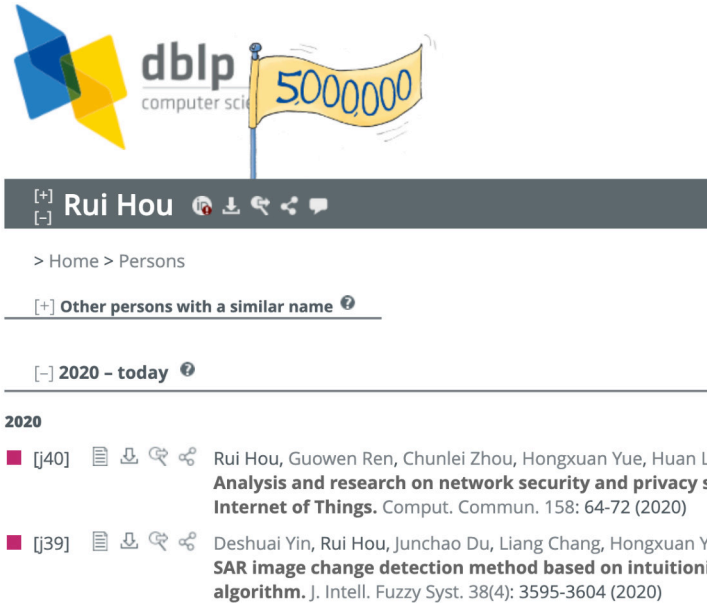
稳住就能赢！坚持才能抄底！

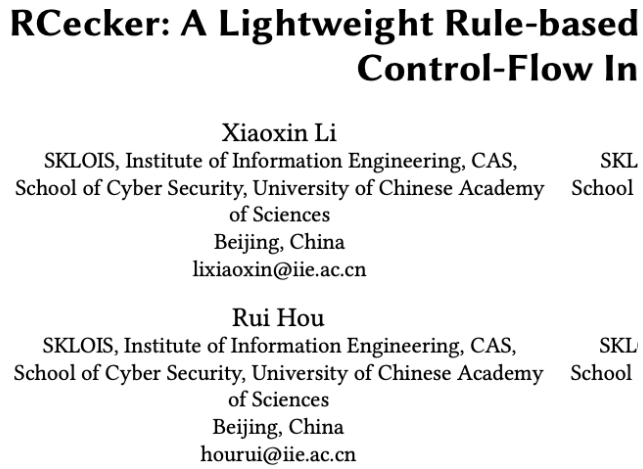
Image (R) source: https://telanganatoday.com/defend-yourself-from-social-engineering-attacks

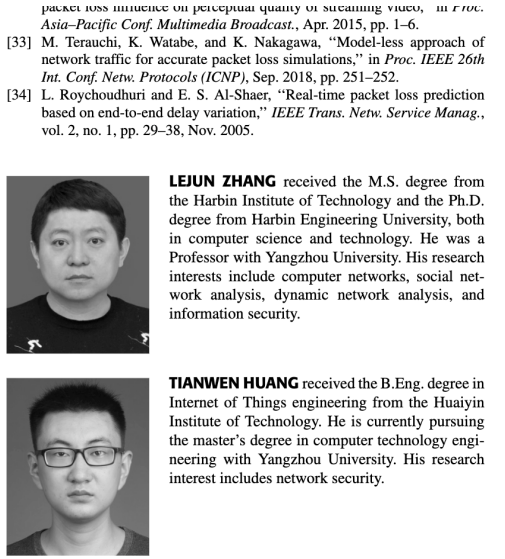
知彼：信息搜集（信息管理）

- 科学使用互联网
- Google hacking
  - 高级操作符
    - filetype:pdf/xls
    - site:xxx.edu.cn
- 找到导师邮箱
  - 学院招生官网
  - 导师个人主页
  - cnki/dblp下载论文

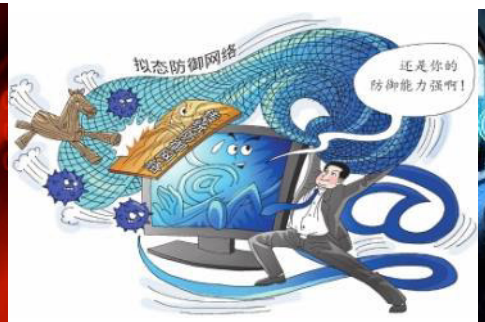






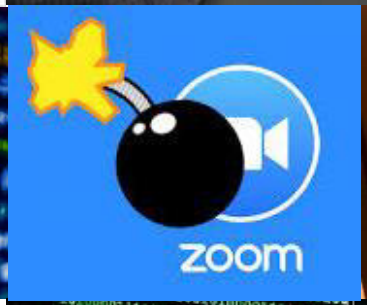


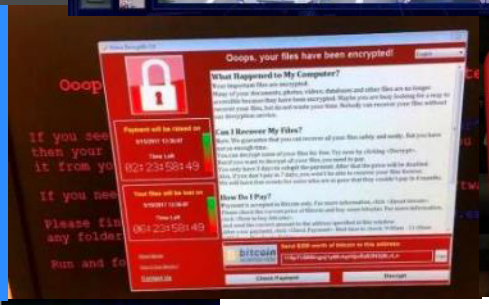
Cyber attacks threaten system security even national security（投资控制）

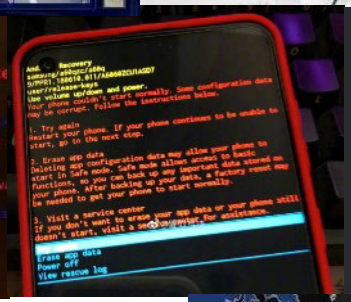



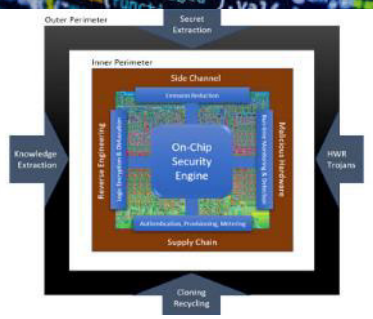










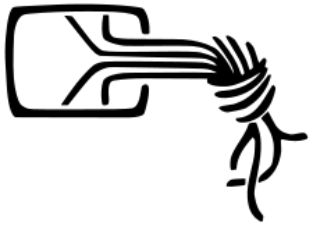




Offense and Defense is a GAME （投资控制）（Cont.）


DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

公安部第三研究所
The Third Research Institute Of Ministry Of Public Security




Worse in Chip (or Micro Architecture) （投资控制） （Cont.）

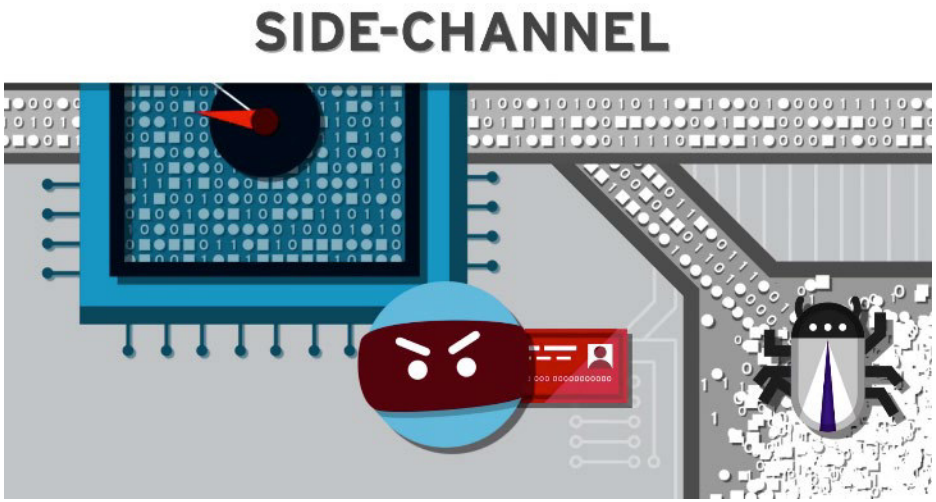
Spectre
v1, v2, v4, v5,
Spectre-BTB,
Spectre-RSB,
ret2spec,
SGXPectre,
SmotherSpectre,
NetSpectre?

Meltdown
v3, v3.1, v3a,
RDCL?

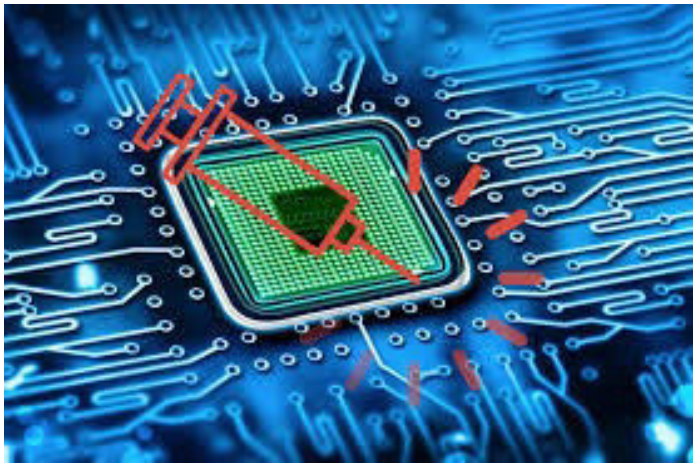
ZombieLoad, MDS?

Foreshadow
Foreshadow-NG,
L1TF?

RIDL, Fallout?



Affected almost ALL CHIPS after 1995



Worse in AI （投资控制）（Cont.）

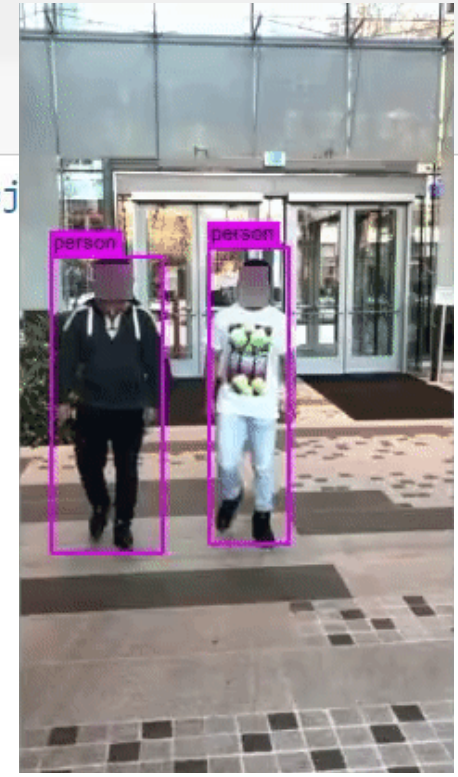
CASE 1:

```
img = PILImage.create(img_c)
img.to_thumb(192)
```

```
https://pbs.twimg.com/media/EqW4Xi1U8AA_KzH?format=j
```

Out[50]:

CASE 2:




```
Is this a boy?: True.
Probability it's a boy: 98.66%
Probability it's a girl: 1.34%
Time cost: 323ms
```

Stealth!

知己知彼，太极生两仪

- 知己：（定位自己）
  - 读研目标：科研 or 工业界 or 事业单位
  - 读研计划：硕士 or 博士；是否出国
  - 研究兴趣：计算机某一个大致的领域
- 知彼：（双选）
  - 核心目标：知道老师邮箱和大致简历
  - 附加：
    - 线上开放学术会议提问
    - 线下“意外”偶遇
    - 搜索得到手机号或微信号
    - （或针对不同老师有一些线上即时交流）

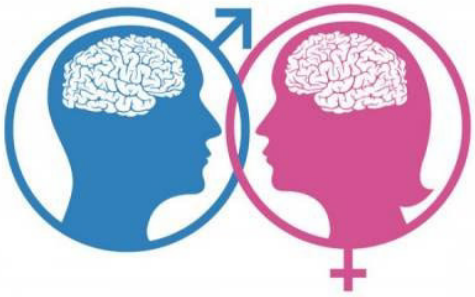


Image source: https://jmc.hksyu.edu/ourvoice/?p=6400

关门打狗，做好简历（质量控制）

- 简历内容太少是不存在的
- 简历一定要突出重点，致力于质量
- 知之为知之，适当包装，符合需求即可
- **模仿大佬简历格式**

个人简历 细节决定成败。 Personal resume

基本信息

姓　名：职业圈　　出生年月：1988.08
民　族：汉　　身　高：166cm
电　话：138****8888　　政治面貌：中共预备党员
邮　箱：9634***@163.com　　毕业院校：职业圈科技大学
住　址：福建省厦门市思明区　　学　历：本科

教育背景

2009.09-2013.07　职业圈科技大学　市场营销（本科）
主修课程：
管理学、微观经济学、宏观经济学、管理信息系统、统计学、会计学、财务管理、市场营销、经济法、消费者行为学、国际市场营销

实习经历

2012.09-2013.06 至今　厦门市职业圈信息科技有限公司　市场营销（实习生）
- 负责公司线上端资源的销售工作（以开拓客户为主），公司主要资源以广点通、智汇推、百度、小米、360、沃门户等；
- 实时了解行业的变化，跟踪客户的详细数据，为客户制定更完善的投放计划（合作过珍爱网、世纪佳缘、56视频、京东等客户）

2013.09-2017.03　厦门市职业圈信息科技有限公司　销售经理
- 负责公司业务系统的设计及改进，参与公司网上商城系统产品功能设计及实施工作。
- 负责客户调研、客户需求分析、方案写作等工作， 参与公司多个大型电子商务项目的策划工作，担任大商集团网上商城一期建设项目经理。

校园经历

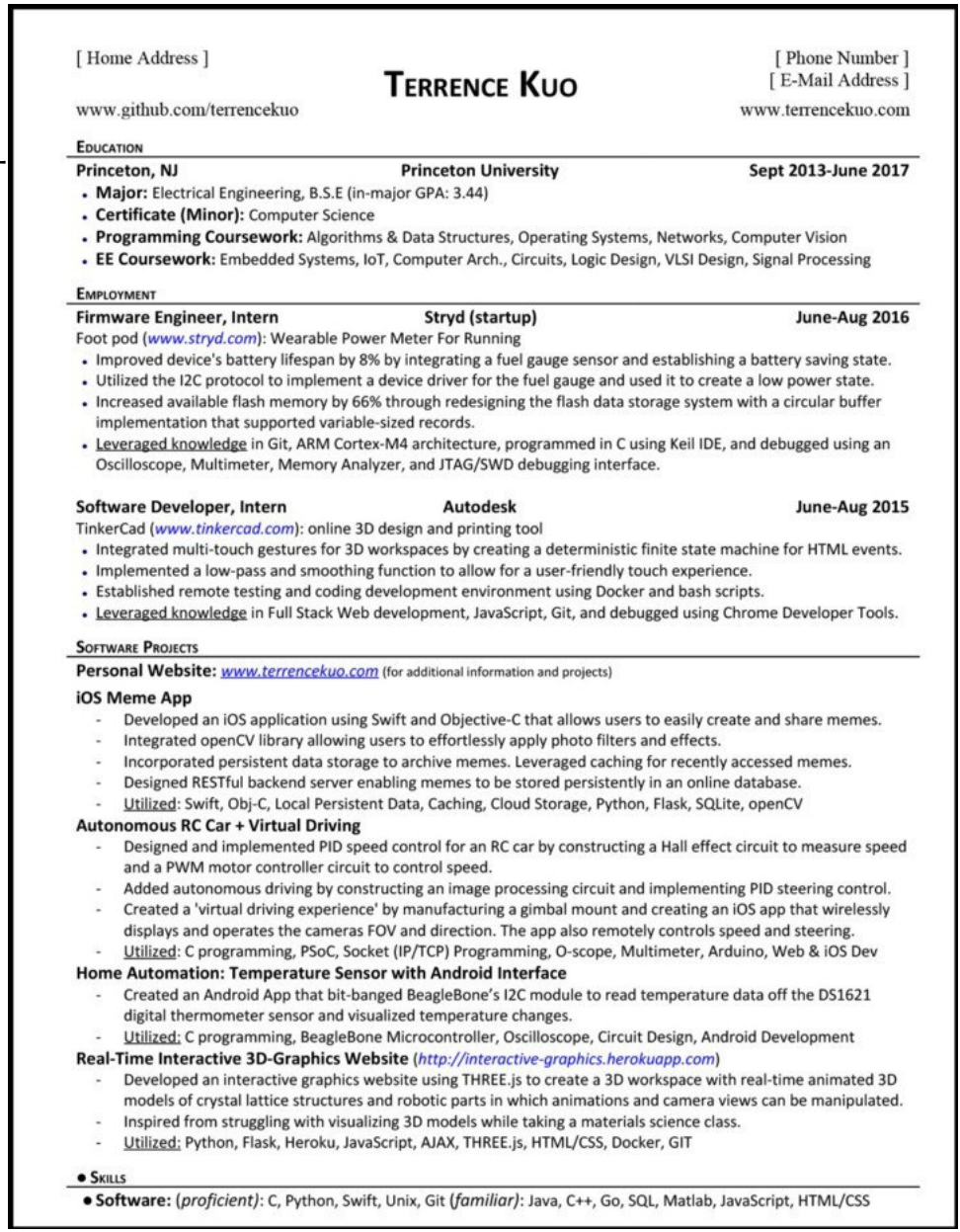
2010.03-2011.06　厦门市 XXXX 有限公司　校园大使主席
- 带领自己的团队，辅助 XXXX 完成在各高校的“XX 计划”，向全球顶尖的 XXXX 金融公司推送实习生资源。
- 整体运营前期开展了相关的线上线下宣传活动，中期为进行咨询的人员提供讲解。后期进行了项目的维护阶段，保证了整个项目的完整性。

技能证书

普通话一级甲等；
大学英语四/六级（CET-4/6），良好的听说读写能力，快速浏览英语专业文件及书籍；
通过全国计算机二级考试，熟练运用 office 相关软件。

自我评价

深度互联网从业人员，对互联网保持高度的敏感性和关注度，熟悉产品开发流程，有很强的产品规划、需求分析、交互设计能力，能独立承担 APP 和 WEB 项目的管控工作，善于沟通，贴近用户。



[Home Address]　[Phone Number]
[E-Mail Address]

TERRENCE KUO

www.github.com/terrencekuo　www.terrencekuo.com

EDUCATION

Princeton, NJ　Princeton University　Sept 2013-June 2017
- **Major:** Electrical Engineering, B.S.E (in-major GPA: 3.44)
- **Certificate (Minor):** Computer Science
- **Programming Coursework:** Algorithms & Data Structures, Operating Systems, Networks, Computer Vision
- **EE Coursework:** Embedded Systems, IoT, Computer Arch., Circuits, Logic Design, VLSI Design, Signal Processing

EMPLOYMENT

Firmware Engineer, Intern　Stryd (startup)　June-Aug 2016
Foot pod (*www.stryd.com*): Wearable Power Meter For Running
- Improved device's battery lifespan by 8% by integrating a fuel gauge sensor and establishing a battery saving state.
- Utilized the I2C protocol to implement a device driver for the fuel gauge and used it to create a low power state.
- Increased available flash memory by 66% through redesigning the flash data storage system with a circular buffer implementation that supported variable-sized records.
- Leveraged knowledge in Git, ARM Cortex-M4 architecture, programmed in C using Keil IDE, and debugged using an Oscilloscope, Multimeter, Memory Analyzer, and JTAG/SWD debugging interface.

Software Developer, Intern　Autodesk　June-Aug 2015
TinkerCad (*www.tinkercad.com*): online 3D design and printing tool
- Integrated multi-touch gestures for 3D workspaces by creating a deterministic finite state machine for HTML events.
- Implemented a low-pass and smoothing function to allow for a user-friendly touch experience.
- Established remote testing and coding development environment using Docker and bash scripts.
- Leveraged knowledge in Full Stack Web development, JavaScript, Git, and debugged using Chrome Developer Tools.

SOFTWARE PROJECTS

Personal Website: *www.terrencekuo.com* (for additional information and projects)

iOS Meme App
- Developed an iOS application using Swift and Objective-C that allows users to easily create and share memes.
- Integrated openCV library allowing users to effortlessly apply photo filters and effects.
- Incorporated persistent data storage to archive memes. Leveraged caching for recently accessed memes.
- Designed RESTful backend server enabling memes to be stored persistently in an online database.
- Utilized: Swift, Obj-C, Local Persistent Data, Caching, Cloud Storage, Python, Flask, SQLite, openCV

Autonomous RC Car + Virtual Driving
- Designed and implemented PID speed control for an RC car by constructing a Hall effect circuit to measure speed and a PWM motor controller circuit to control speed.
- Added autonomous driving by constructing an image processing circuit and implementing PID steering control.
- Created a 'virtual driving experience' by manufacturing a gimbal mount and creating an iOS app that wirelessly displays and operates the cameras FOV and direction. The app also remotely controls speed and steering.
- Utilized: C programming, PSoC, Socket (IP/TCP) Programming, O-scope, Multimeter, Arduino, Web & iOS Dev

Home Automation: Temperature Sensor with Android Interface
- Created an Android App that bit-banged BeagleBone's I2C module to read temperature data off the DS1621 digital thermometer sensor and visualized temperature changes.
- Utilized: C programming, BeagleBone Microcontroller, Oscilloscope, Circuit Design, Android Development

Real-Time Interactive 3D-Graphics Website (*http://interactive-graphics.herokuapp.com*)
- Developed an interactive graphics website using THREE.js to create a 3D workspace with real-time animated 3D models of crystal lattice structures and robotic parts in which animations and camera views can be manipulated.
- Inspired from struggling with visualizing 3D models while taking a materials science class.
- Utilized: Python, Flask, Heroku, JavaScript, AJAX, THREE.js, HTML/CSS, Docker, GIT

SKILLS

- **Software:** (*proficient*): C, Python, Swift, Unix, Git (*familiar*): Java, C++, Go, SQL, Matlab, JavaScript, HTML/CSS

包装打磨，釜底抽薪

- 这段时间应该做的事
  - 打磨简历（用下面做的事包装）
  - **套磁、信息搜集不可少**
- 可以做的事：
  - 玩
  - 学习一个完整工程项目
  - 学习一些算法与底层知识
  - 读一些英文论文
  - 跟进某领域工业界进展
  - 了解计算机各领域发展
  - 了解计算机早期发展历史
  - 锻炼聊天与对话技能

运气是争来的（沟通协调）

- **如果有把握过线，现在就可以发邮件**
- 把握考场优势
- 积极的心理暗示
- 眼观六路 耳听八方 胆大心细
- 准备要充分，很多东西网上都能查到
- 做一些标准的、体现科研能力的事情
- （无低级错误，符合审美的）
- **复试的过程本质上是沟通协调的过程**
- **做题思维不太可取，要对话思维**
- 雄关漫道真如铁 苍山如海

投其所好：套磁，提前对话

- 任何时候都可以套磁
- 态度要诚恳，表达要诚实
- 简历要做得简洁规范，一定要有读研规划（包括是否读博）
- 每个老师都套是可以的
- 最后有了结果最好再说明回复下回复过你的老师（我已录取到xx老师，感谢信任）

一志愿学生自荐-xx-300分学硕-本科xx-项目经验丰富/基础尚可-……

X老师您好，

我叫xx，来自xx，多次奖学金，有某国赛/省赛x等奖，对您和您团队目前正在研究的xxx方向感兴趣，并已*拜读您xxx的论文*，我在xxx方向曾经**学过xxx基础**，**做过xxx相关工作**，希望有机会能向您学习，附件是我的简历和读研计划等，谢谢。

敬礼！

学生xx

安全管理

- 和老师交流时，谨慎吹牛，特别是面试时。
- 套磁不要出现张冠李戴等低级错误
- 说谎必然会付出代价

你打你的，我打我的（把握个性）

- 不用过多比较他人，做好自己
- **简历和对话过程中显示出个性**
- **不怕拼命怕平凡**
- **如何彰显自己的与众不同**
  - ▶格式规矩
  - ▶**内容靠谱**
  - ▶**有自己的实践及思考（体现科研能力）**

再润色

套磁成功，老师回复了

- 如不是礼貌性回复：成功的几率很大
  - 进一步对话：询问你的学习科研经历等等 -> 如实回答（基本稳了）
  - 目前不清楚具体名额 -> 保持联系
- 礼貌性回复：看情况仍可让老师推荐或感谢
  - 没名额
  - 祝好
  - 咨询招生办
  - 机会不大

套磁失败，老师无回复

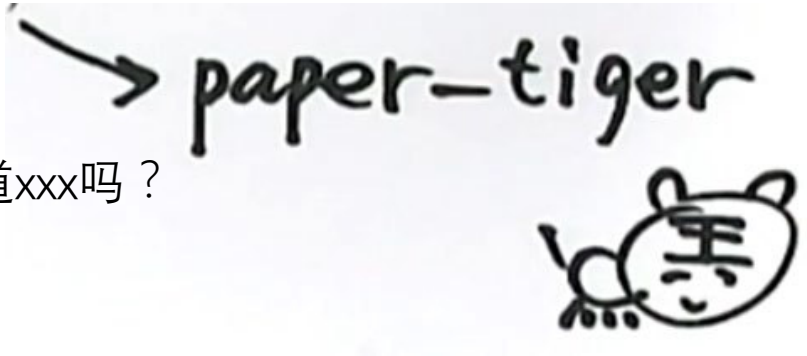
- 再润色简历、邮件正文等咨询下一个老师
- 连续几个不回复：
  - 放轻松
  - 面试时积极发挥

面试自我介绍，开启对话

- 围绕简历
- 英文自我介绍：
  - 叫什么，家在哪，毕业院校
  - 荣誉和实践经历（简历上的）
  - 感兴趣的研究方向，了解了什么
  - （有和xxx老师邮件等交流过，有何感想）
  - 大致的读研计划
  - 诚挚感谢
- 五分钟
- 用词不用太难，让人一耳能听懂即可
- 相对流畅
- 建议背稿
- 要有眼神交流，必要可手势

对话聊天常见内容

- Please introduce yourself briefly?
- What was the most unforgettable thing during your undergraduate ?
- 计算机网络的TCP协议和UDP协议的区别？
- Java中接口和抽象类的作用？
- 数据库事物的ACID属性指的什么？
- 你的倾向于学硕还是专硕？你能接受转到专硕吗？你有想过读博这件事吗？
- 你为什么报考xxx？
- 你的家乡在哪里？你认为xx城市和xx城市相比如何？
- 你简历上写的做过xxx项目具体负责了哪些内容？
- 你简历上xxx奖是什么？
- 你熟悉Linux吗？
- 最近在做什么？毕业设计完成情况如何？
- xxx课程你学的怎么样？还记得哪些？知道xxx吗？
- 你业余时间做什么？有何爱好？



没有真题！没有标准答案！都是纸老虎，记住是对话，不要慌，有主见

应变，趋利避害（变更管理）

- 复试对话中，
- 遇到清楚的问题回答方案：
  - xx是计算机某领域基础知识，在xx上有应用，我简历上的某项目/某课设曾了解使用过，我主要做了xxx，结果xxx
- 遇到不会的问题回答方案：
  - xx没有了解过，不过您可能是想问xx技术/xx概念，我简历上某项目曾做过xxx，似乎也能符合这个需求
  - 我主要做了简历上的xxx，您问的xxx我不太了解，这是哪个相关的技术
- 遇到非技术问题回答方案：
  - 聊天，拉家常，说最近读了xx论文，做了哪些准备

围绕自身经历、提出解决方案、结合简历是关键

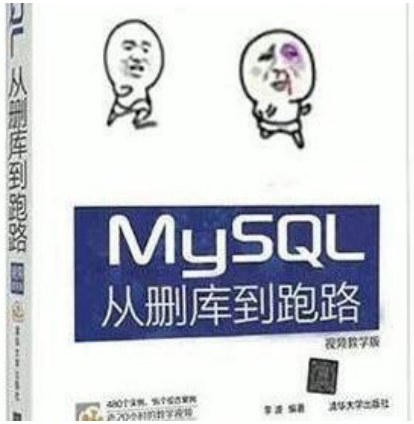
再攻心（合同管理）

- 复试结束后，
- 根据复试表现情况以及老师们的态度和气氛，
- 1天内适当再发一封邮件
  - **两点：**
    - **一是询问结果**
    - **二是再肯定自己不会跑路**

必要几手准备！有书读！准备其他的步骤一致。

你就是下一个天选之人

人，一定要有梦想



从今以后，黑客与我无关，数据已删，shell已转手，肉鸡已放完，日常搞站的电脑已经砸了；从前没得选择，如果一切可以重新开始，我只想做个好人！

I. 坚持才能抄底 —— 今年形势依旧有利，机会很大

II. 知己知彼，关门打狗 —— 做好简历，选择合适的

III. 包装打磨，釜底抽薪 —— 利用这段时间学习后再包装

IV. 运气是争来的 —— 要主动出击

V. 投其所好 —— 套磁得法，提前开启对话

VI. 你打你的，我打我的 —— 心无旁骛，做好自己

VII. 再润色 —— 根据套磁情况，再突出个性，与众不同

VIII. 应变，趋利避害 —— 面试时把握对话节奏

IX. 再攻心 —— 复试后仍不失主动

祝一切顺利 牛年大吉

感谢批评指正

THANKS