# 前沿知识考核.

以下3选1即可, 开学前一周完成答辩, 准备好了可以联系我, 即使在暑假, 也可以在线答辩.

1. 1-3人一组, 解读顶级论文.

要求如下:

1. 论文源自近3年顶级会议或者期刊.

会议

* IEEE Symposium on Security and Privacy
* ACM Conference on Computer and Communications Security
* European Cryptology Conference
* International Cryptology Conference
* Usenix Security Symposium

期刊

* IEEE Transactions on Dependable and Secure Computing,
* IEEE Transactions on Information Forensics and Security,
* Journal of Cryptology JACM
* Journal of the ACM
* 其它IEEE Transactions 系列或者ACM Transactions系列期刊

1. 简单的英译汉和复制粘贴不得分.
2. 提交的报告必须自包含, 使得明年研一的同学看得懂听得懂, PPT可以被纳入明年区块链课程. 因此
3. 不要面面俱到, 而要抓住论文的核心贡献和技术.
4. 可能需要补充论文省略掉的数学推导和背景知识.不能以“论文就是这样写”的敷衍.
5. 选择的目标论文, 请7.11日前, 在线文档中登记.
6. 1-3人一组, 解读知名区块链的白皮书.

要求同上, 唯一不同的解读对象是知名的区块链, 例如, Facebook数字货币Libra, 斯坦福大学的Findora.

1. 1-3人一组, 写一篇论文.

排版结构的要求与期刊论文相同, 要有创造性, 即与已有的工作不一样. 创造性可以小, 但是必须有, 不得抄袭.