课程小论文

挑选一篇从2015年-2025年的CRYPTO、EUROCRYPT、ASIACRYPT、CCS、S&P会议上的密码学相关论文（必须带有安全性证明），写一篇读书笔记

- 要求
  - 详细介绍文章的背景、贡献
    - 需要阅读文章的related work，确定文章背景与贡献
  - 详细介绍文章的方案构造细节，并加入融入自己的理解
  - 仔细阅读论文的安全性证明，并对证明（思路）进行总结
  - 指出文章可能的未来研究方向
  - （选做）改进文章中的方案，或应用相关方案，拓展成一篇小论文
  - 读书笔记要尽可能完备，确保上过本门课的同学能够读懂
  - 读书笔记提交格式为pdf，中英文均可，**需要使用LaTeX撰写**
- 截止日期：2025年12月31日23：59
- 提交邮箱：liuyi@jnu.edu.cn