首先得做一个自我检讨，其实这个问题暑假的时候就已经存在了，我也意识到了。有时候会想当然的活在自己的世界里，我以为的并不会是别人以为的，我想的并不是别人能够理解的。会换位的想，如果我是老师，我是其他的人，这也会让我觉得这样的做法会同样让我心里很不爽。现在能够意识到问题的严重性，我会改正的，老师要相信我啊。

今日工作：

1. 下午it伦理课；晚上政治课；
2. 今天看了一篇有效的无证书聚合签名方案，无证书签名解决了密钥托管和证书管理的问题，聚合签名降低了验证代价和缩短了签名的长度；了解了无证书的签名过程大致包括系统生成，部分私钥生成，签名，验证等阶段；对这篇论文的安全性证明和以前的所看论文中证明差不多，但是还是不够理解。同时不理解为什么无证书签名在随机预言机模型下是不安全的？而在标准模型下证明能够提供更充分的保证？
3. 接下来，将继续看关于无证书签名方面的论文，并且深入去读；