1. 分组密码上课收获：

上次发了两篇论文：

一篇是使用双线性对的高效签名方案，本方案是在预言机模型下，假设是K-CAA问题展开的。

另一篇是基于强壮的RSU假设展开讨论的，本方案是在无预言机模型下。

在这两篇论文的假设中知道了假设的区别，分为：简单假设（也是若假设，标准假设），这种假设较好于强假设，强假设算是一种不太合理的假设，有时这些假设是动态的，交互式的。

然而我们追求的是静态假设，标准假设，越简单越好。

假设对于写证明部分是很重要的，基本上假设越简单需要的可证明安全性难度相对大一些。

从这两篇论文中可以看到A篇论文中有很多假设，看论文的时候我看的有点绕，知道每一个假设的定义以及假设之间的对等关系，但是不明白作者为什么要写这么多，后来老师讲一篇论文基本上只有一个最核心的假设，其他假设都是次要的（没有那么重要），需要把最核心的假设与证明作为重点看。除此之外我也很疑惑论文的主题之外也有讲很多其他的，仔细看了一下标题是后面有（以及应用），那是这种方案的一个扩展，这样弄清楚每一部分的存在意义就知道本篇论文的重点所在，而不是眉毛胡子一起抓，到最后时间也花了最后也什么都没有懂。

其中不足是在课堂上并没有听懂可证明安全分析部分，课下晚上又继续看了论文核心部分难点部分。

1. 之前看的是普通的隐私保护消息认证，计划下面看一下2003年提出的无证书签名的是如何实现的隐私保护的。