今日工作：

1. 上午英语，下午人工智能，晚上组会；
2. 今天没有去读新的论文，把这几天读的两篇论文给梳理了一遍。

一篇是未使用对的无证书聚合签名，对该方案的八个算法在纸上梳理了一遍，但是还是不能做到不看论文，将这个八个过程按照流程给推一遍。在安全性证明这一块，给了无证书签名和无证书聚合签名的证明过程，知道其安全性是基于ECDP问题的解决能否，但是对其每一步的证明流程还是不知道怎么弄的。

另外一篇是加强基于身份批验证的安全与隐私的方案，和上一篇存在一样的问题。

3.接下来的工作：安全性证明一直是我不会的地方，还有就是觉得自己看论文一知半解，以至于都提不出一些像样的问题，想接下来能够好好研读每一篇论文。