1. 2003年第一次提出的无证书这篇论文粗略的看，刚开始准备还没有什么进展。
2. 开了车联网小组会。汇报人汇报的论文是那篇我之前看过的Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs，汇报的很清楚，针对之前老师您提问的问题我对论文进行的思考对我很有帮助，多谢老师！

小组收获：

1. 在组会中有师兄师姐提出了更加具体的问题，也有更加基础的问题，比如说：论文中用到的哈希函数的作用、证书撤销列表的作用、私钥与公钥具体作用是什么、签名的作用是什么、加法群与乘法群的区别是什么以及什么是有限域、加法群与乘法群在占用内存上的区别、DSRC协议具体是什么（这些不能说只是别人用我们也用，要真正的明白理解一些概念为什么才可以写出属于自己的好论文），针对这些问题，我搜索一下，并记下笔记，加深印象，让理解更透彻，现在这个阶段基础是不可忽略的！
2. 论文中使用了双线性对，可以用椭圆曲线去替代它吗？这是我之前没有思考过的问题，双线性对有对称的与非对称的，哪种容易转换等，这些需要进一步了解。
3. 使用双线性对开销大，有时在想是不是现在的一种趋势是使用的很少了，不需要去看这种双线性对的论文了，其实不是，双线性对是保证了一个安全性，在安全与效率面前，安全是最重要的。
4. 实验数据如果引用别人的需要标注，最好自己实验。
5. 针对2中的问题，其实一篇论文中可以有很多需要学习的知识与扩充的点，针对这些进行思考，思考不出来进行百度查阅资料等，之后这些东西就变成自己的知识。所以看论文的目的不单单是看论文本人，还要针对论文中的内容进行拓展扩充。除此之外要分析论文中的贡献与缺点，汇报的时候在PPT中也是需要有的部分，有自己对论文的理解在里面。这个通过查看别人对此篇论文的引用可以知道本文的缺点，这样可以看到是从哪个方面去分析的，培养这种批判性的思维方式，并对此论文怎样改写更好。
6. 晚上有课，计划下一步对小组会提出的问题进行百度，确定了方向，下一步看师姐给发的一篇论文：A Threshold Anonymous Authentication Protocol for VANETS.