Chapter Wise Evaluation

Chapter 1:

简介中介绍了选题的背景和意义，同时详细介绍了密码学、公钥密码学、签密和密码分析的研究现状。之后简要介绍了论文的主要创新点和论文结构。作者在当前已有的签密方案的基础上，作者提出几种基于椭圆曲线的签密方案的分析与改进，提高签名方案的安全性。论文的选题选题具有研究意义，参考文献收集详实，论文结构设计清晰，有较强的逻辑性。

Chapter 2:

作者详细介绍了支撑研究所需的数学基础知识。现代密码方案大多数都是基于代数和数论，作者介绍了密码方案相关的定义和概念。

Chapter 3:

作者介绍了密码学的研究现状。作者详细介绍了密码学分类和数字签名、基于椭圆曲线的密码系统、签名后加密、签密以及密码学分析原理。

Chapter 4:

针对基于椭圆曲线的防火墙签密方案进行详细的密码分析，考虑该方案存在的安全性问题，作者提出一个改进方案提供更好的安全性。

Chapter 5:

针对基于椭圆曲线的盲签密方案进行详细的密码分析，证明当前方案存在验证的安全漏洞。作者提出一个改进方案提高了安全性。

Chapter 6:

针对基于超椭圆曲线的盲签多文档方案进行详细的密码分析，证明其方案存在安全问题，并且不能满足盲签密的安全需求。针对原方案不具备伪造攻击抗性的问题，作者提出一个改进方案提高安全性。通过详细分析改进方案的安全性，证明改进方案能够满足较好的安全性。

Chapter 7:

作者提出一种基于椭圆曲线的多接收者聚合签密方案，同时在此基础上为不同的场景提出不同的版本。新方案具有很好的安全性，且更加的高效。

Chapter 8:

作者给出了不同签密方案的安全性分析，并且针对当前存在漏洞的方案进行改进提高安全性。在当前的研究工作的基础上，提出未来继续的研究工作。