作为离散数学研究性学习小组的组长，我带领六人小组深入研究了同态加密在联邦学习中的应用发展。研究始于对同态加密和联邦学习的简介，通过 YouTube 等视频平台的面向大众的科普视频为小组成员提供了初步理解。

小组快速掌握了同态加密的核心概念，着重研究了与联邦学习相关的加密算法，特别关注不同算法的特性和适用场景，以优化在联邦学习环境中的应用。随后，我们利用谷歌学术平台深入研究同态加密在联邦学习中的应用发展。

六人小组的任务分配如下：

俞乐楠（RSA 算法）：深入研究 RSA 算法，基于大整数分解困难问题，满足乘法同态特性。

傅裕翔（CKKS 算法）：探讨 CKKS 算法，基于离散对数困难问题，具备公钥加密和数字签名功能，满足乘法同态特性。

徐文彬（Paillier 算法）：研究 Paillier 算法，基于合数剩余类问题，是目前最为常用和实用的加法同态加密算法。

袁昊旻（Boneh-Goh-Nissim 方案）：深入了解 Boneh-Goh-Nissim 方案，支持任意次加法同态和一次乘法同态运算。

赵会洋（Gentry 方案）：追溯全同态加密算法的发展历程，关注于 Gentry 提出的方案以及后续方案如何基于格代数结构构造。

董伟（BGV 方案和 BFV 方案）：研究 BGV 方案和 BFV 方案，这两种全同态加密算法已在主流同态加密开源库中实现。

通过小组成员的努力学习和深入研究，我们对同态加密在联邦学习中的应用有了更为全面和深刻的理解。这份研究性学习报告为我们奠定了在这一领域深入研究的坚实基础。