在本次研究性学习中，我主要负责BGN算法部分的研究。BGN作为半全同态加密的关键算法，起到十分关键的过渡作用。但在全同态算法日渐完善的今天，BGN可以发挥作用的舞台也逐渐减小，但在部分特殊情况下，BGN算法可以用最少的资源、最高的效率完成自己的任务。联邦学习作为一个近年才热火的话题，其留给BGN施展拳脚的空间更是狭小，分析BGN算法的主要优势以及在何情景下才能发挥最大优势便是我的主要任务。这对我来说是一大挑战——我对同态加密和联邦学习的了解十分少，加之目前已有的BGN相关文献便已屈指可数，更何况与联邦学习相关的参考文献。因此我在文中提出的分析大多出于自己对BGN算法的理解，可能不太准确，还望海涵。