

摘要

本报告主要介绍安全多方计算的定义，实现安全多方计算加法和乘法的具体方式，然后使用这些协议来实现神经网络的隐私学习和 GWAS 的隐私计算。