用于安全神经网络推理的高效隐私保护方案

陈立全[1,2]，杨紫瑄[1]，张鹏[1]，马旸[1]
[1]东南大学网络空间安全学院，中国南京市，210096
[2]紫金山实验室，中国南京市，211189

摘要：随着智能设备和云服务的广泛应用，加之本地计算与存储资源受限，大量用户倾向于将私有数据传输至云服务器进行处理。然而，敏感数据以明文形式传输引发用户隐私与安全方面的担忧。为应对这些问题，提出一种基于同态加密与安全多方计算的高效隐私保护安全神经网络推理方案，该方案在确保用户与云服务器双方隐私的同时，实现了快速准确的密文推理。首先，将推理过程划分为3个阶段：调整网络结构的合并阶段、执行同态计算的预处理阶段以及隐私数据秘密共享的浮点运算在线阶段。其次，提出一种网络参数合并方法，以降低乘法层级的成本，并减少密文—明文乘法与加法运算次数。最后，提出一种快速卷积算法，以提升计算效率。与其他最先进的方法相比，所提方案在线阶段的线性操作时间至少减少11%，显著降低了推理时间和通信开销。

关键词：安全神经网络推理；卷积神经网络；隐私保护；同态加密；秘密共享
https://doi.org/10.1631/FITEE.2400371