CKKS是一种高效的全同态加密方案，其支持对浮点数近似计算，通过 SIMD (Single Instruction Multiple Data)技术可以将多个明文打包为单个密文，同时对多个比特处理，提高加密与解密的效率。具体而言，CKKS主要包含以下几个函数：

keyGen(λ)：密钥生成函数，输入一个安全参数λ，输出公私钥对(pk, sk)和一个辅助计算密钥evk;

Enc(pk, m)：加密函数，输入公钥pk和明文m，输出加密后得到的密文c:

Dec(sk, c):解密函数，输入私钥sk 和密文c，输出解密后得到的明文m；

Add(c1,c2)：密文加法函数，输入两个明文m1,m2,对应的密文c1.c2,输出m1+m2,对应的密文Cadd:

Mult(c1,c2,evk)：密文乘法函数，输入两个明文m1, m2, 对应的密文c1,c2,以及辅助计算密钥evk，输出m1×m2,对应的密文Cmult.

CKKS是目前唯一一个支持浮点数运算的全同态加密方案，允许对实数或复数的浮点数进行加法和乘法的同态运算。此外，相比于其他同态加密方案，CKKS 具有高效的加解密、较小的密文大小等优势，非常适合用于隐私保护的机器学习。

以下为一个利用CKKS乘法性质高效处理联邦学习问题的应用：

联邦学习中，计算损失函数是一个重要环节，而传统的Paillier算法中，需要泰勒展开以计算近似损失函数，计算量大。而基于CKKS同态加密的优化方案可以改善这个问题，CKKS加密方案是基于LWE困难问题的同态加密方案与Paillier同态 加密方案相比，此加密方案保有加法同态性质以及有限次乘法同态性质，使得加密结果不会出现影响训练结果的误差。 若双方的向量内积计算有两个，参与方A，B各有 一个向量VA ={ a0，a1，...，an }，VB ={ b0，b1，...，bn }，要求 计算两个向量的内积，且不泄露各自的隐私 A 使 用 自 己 的 公 钥 （CKKS 算 法） 加 密 数 据 EncA (VA )，将密文发送给B；B用A的公钥 （CKKS算 法） 加密数据EncA (VB )；B计算C0=EncA (VA ) EncA (VB )= EncA (a0·b0 )，…，EncA (an - 1·bn - 1 )；B对C0移位 n/2 得到C0'， 求和得C1 =C0 +C0'；B对C1移位 n/4 得到C1'，求和得C2； B得到最终结果，将其发送给A；A解密得到结果。CKKS可以使用公式直接对加密 参数θ和数据( x，y )进行运算。CKKS引入rescaling，使 同态计算期间，编码前后的消息大小保持基本不变， 保证方案所需的最大密文模数随运算电路深度呈线性增长，极大地提高方案的效率。

结果表明，采用CKKS加密方案可以节省时间， 在保证用户隐私的情况下达到近似的准确率，但方案仍存在一定不足，针对用户数据方面，参与方所提供的数据质量较差会影响训练效率；用户在参与过程中掉线，可能无法得到想要的效果。未来将在解决数据异质性以及鲁棒性上进行进一步的研究，考虑进一步提升计算效率。