Práce se zabývá odvětvím kryptografie zvaným bezpečné sdílené počítání, což je technika, která umožňuje více stranám spolupracovat na výpočtu jediné funkce tak, že její vstupy zůstanou utajeny. Konkrétněji se práce zabývá bezpečným sdíleným počítáním nad okruhem celých čísel modulo p^k. Práce začíná představením obecného principu protokolů pro bezpečné sdílené počítání, po kterém následuje vybudování potřebné teorie nad komutativními okruhy, která bude v poslední části práce potřeba k popisu a pochopení konkrétního protokolu.