Táto práca sa zameriava na konštrukcie homomorfných schém na zdieľanie tajomstva (HSS), o ktorých nie je známe, že by implikovali plne homomorfné šifrovanie. Efektivita týchto konštrukcií závisí na zložitosti problému distribuovaného diskrétneho logaritmu (DDLog) v odpovedajúcich grupách. Tento problém detailne popisujeme, zameriavajúc sa na možnosť využitia predspracovania v grupách prvočíselného rádu a na odvodenie horných medzí pre pravdepodobnosť úspechu pre DDLog problém s predspracovaním v generickom grupovom modeli. Ďalej predstavujeme novú konštrukciu HSS. Našu konštrukciu zakladáme na Joye-Libert šifrovacej schéme, ktorú prispôsobíme tak, aby podporovala efektívny protokol pre distribuovaný diskrétny logaritmus. Naša modifikovaná Joye-Libertova schéma vyžaduje novú množinu bezpečnostných predpokladov, ktoré uvedieme, dokazujúc IND-CPA bezpečnosť našej schémy za týchto predpokladov.