Algebraická kryptoanalýza je metoda používaná v kryptografii k analýze a prolomení kryptografických systémů a algoritmů. Spočívá ve vyjádření vztahu mezi otevřeným textem, šifrovým textem a klíčem, systémem polynomiálních rovnic, a poté řešením systému pomocí Gröbnerových bází. Pokud navíc rovnice závisí pouze na klíči, můžeme vygenerovat více systémů pro různé páry otevřených a šifrovaných textů.

Tato práce se zabývá technikami předzpracování v algebraické kryptoanalýze, které redukují velké systémy polynomiálních rovnic, aby zlepšily výkon řešících algoritmů. Zaměříme se na techniku, která si klade za cíl zvýšit řídkost polynomů, a položíme teoretické základy pro dvě různé metody. První metoda spočívá v důkladném procházení všech dvojic, kdežto druhá metoda využívá Locality-Sensitive Hashing pro hledání kandidátů na podobné polynomy. Na závěr se pokusíme zlepšit tuto druhou metodu cílením pouze na největší monomy v polynomech.