Tato diplomová práce se zabývá schématy polynomiálních závazků, což jsou schémata umožňující vytvářet polynomiální závazky a následně pomocí spuštění navrženého protokolu důvěryhodně vyhodnocovat polynomy v požadovaných bodech.

Jako náš hlavní výsledek navrhujeme nové schéma, které umožňuje pracovat s polynomy více proměnných a efektivně dokazovat korektnost vyhodnocení polynomu ve více bodech.

Vytvoření našeho schématu vedlo k využití poznatků z teorie algebry, především zabývající se vlastnostmi ideálů v polynomiálních okruzích a grupovými vlastnostmi.

V porovnání s jiným schématem, které je též navrženo pro polynomy více proměnných, se nám podařilo zlepšit komunikační složitost během protokolu.