Zero-knowledge SNARKy se v poslední době staly velmi studovaným kryptografickým tématem zejména díky jejich využití v kryptoměnách. Většina z těchto protokolů je tvořena za pomoci schémat pro závazek k polynomu jako je například KZG protokol vytvořený Katem, Zaveruchou a Goldbergem (ASIACRYPT 2010). Všechny důkazy extrahovatelnosti KZG protokolu byly však až do nedávna buď v idealizovaných modelech nebo za příliš silných předpokladů. Až letos Lipmaa, Parisella a Siim (EUROCRYPT 2024) dokázali extrahovatelnost závazku v KZG protokolu ve standardním modelu za předpokladu jejich nové podmínky ARSDH.

V této práci navazujeme na článek Lipmaa a spol. a dokazujeme speciální solidnost pro verzi KZG protokolu s polynomem o dvou proměnných. Za tím účelem generalizujeme jejich předpoklad ARSDH a definujeme speciální solidnost pro verzi KZG protokolu se dvěma proměnnými. Následně dokazujeme, že verze KZG protokolu se dvěma proměnnými dosahuje speciální solidnosti za předpokladu ARSDH podmínky a naší nové zobecněné ARSDH podmínky. Nakonec přinášíme podrobnější analýzu času běhu extraktoru od Lipmaa a spol.