Zero-knowledge SNARKs have become an extremely studied topic in cryptography due to their recent applications in modern cryptocurrencies. Most of these protocols are created using Polynomial Commitment Schemes such as the KZG protocol by Kate, Zaverucha, and Goldberg (ASIACRYPT 2010). Until recently, the known proofs of extractability of the KZG protocol were either in idealized models or under very strong assumptions. This year, Lipmaa, Parisella, and Siim (EUROCRYPT 2024) proved the KZG protocol to be Special Sound and Black-Box Extractable in the standard model under their new ARSDH assumption.

In this thesis, we build upon the work of Lipmaa et al. to prove Special Soundness for the bivariate version of the KZG polynomial commitment. To this end, we generalise their ARSDH assumption and define Special Soundness for the Bivariate KZG polynomial commitment. We then prove that the Bivariate KZG polynomial commitment achieves the Special Soundness under the ARSDH assumption and our generalisation of the ARSDH assumption. Finally, we give a more refined analysis of the running time of the black-box extractor from Lipmaa et al.