This thesis focuses on polynomial commitment schemes – cryptographic protocols that allow committing to a polynomial and, subsequently, proving the correctness of evaluations of the committed polynomial at requested points.

As our main results, we present new schemes that enable committing to multivariate polynomials and efficiently proving the correctness of evaluations at multiple points.

As the main technical tools for our constructions, we use theorems from abstract algebra related to ideals of polynomial rings and some group-theoretic properties.

Compared to the state-of-the-art that inspired our work, our main contribution is the improved communication complexity achieved by our protocol.