

This thesis studies batch Proofs of Exponentiation (batch PoE). We explore existing batch PoEs and analyze their verification cost. We also introduce two batch PoEs and compare their performance with the performance of the existing approaches. Our batch PoEs outperform the existing ones, both in theory and in practice. We achieve the improvement in the verification costs by decreasing the expected number of group multiplications. For the practical analysis, we choose the values of the protocol parameters as used in practice, and then measure the time of multiplications and exponentiations on the verifier's side of the discussed protocols in our implementation in C++.