Abstract:

We construct a delegation scheme for delegating polynomial time computations. Our scheme is publicly verifiable and non-interactive in the common reference string (CRS) model. The soundness of our scheme is based on an efficiently falsifiable decisional assumption on groups with bilinear maps. Prior to this work, publicly verifiable non-interactive delegation schemes were only known under knowledge assumptions (or in the Random Oracle model) or under non-standard assumptions related to obfuscation or multilinear maps.

In addition, our scheme has two desirable features: The proofs are unambiguous, in the sense that it is hard to find two distinct proofs for the same statement, and are updatable in the sense that given a proof for the statement that a Turing machine \( M \) transitions from configuration \( C_0 \) to \( C_T \) in \( T \) steps, one can efficiently generate a proof for the statement that \( M \) transitions from configuration \( C_0 \) to \( C_{T+1} \) in \( T+1 \) steps.

We show that such a delegation scheme implies PPAD hardness, by following a similar approach to that of Choudhuri et al. (STOC2019), who obtained PPAD hardness based on an assumption related to the soundness of the Fiat-Shamir paradigm.

This is based on two joint works, both with Omer Paneth and Lisa Yang.