# Delegable zk-SNARKs with Proxies

**Jinrui SHA, Shengli LIU**

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2782-9

# Problems & Ideas

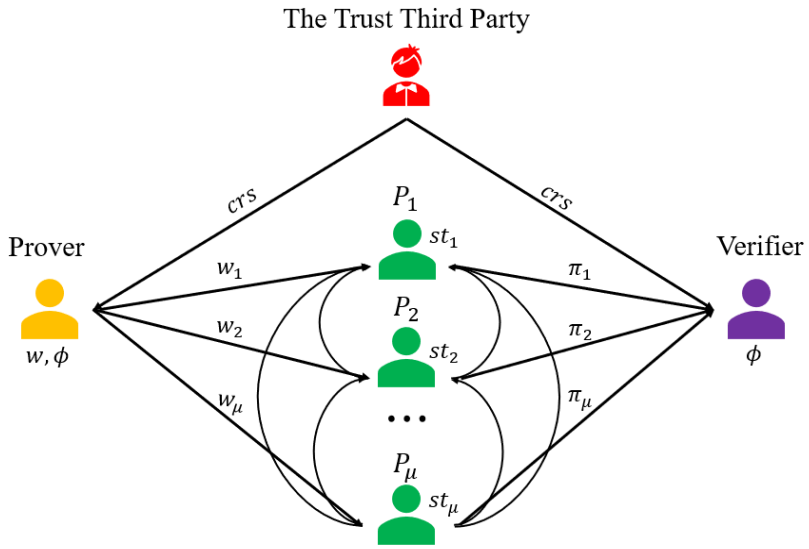
- **Problems :**

  Is it possible for the prover of zk-SNARK to delegate the proving ability without leaking the witness?

- **Ideas:**

  On the one hand, the proxy has to use the witness to delegate the proof generation; On the other hand, the proxy is not allowed to obtain the witness to avoid information leakage.

  Each proxy only gets a piece of the witness, which alone does not leak information about the witness. But many proxies can cooperate to finish the generation of the proof.



# Main Contributions

- **Contributions:**
  - We define the syntax of $(\mu, k, k', k'')$-delegable zk-SNARK and its $k$-completeness, $k'$-knowledge soundness and $k''$-perfect zero knowledge.
  - We construct a $(\mu, 2t+1, t, t)$- delegable zk-SNARK for the NPC language of arithmetic circuit satisfiability, which is further characterized by the quadratic arithmetic programs relation $R_{QAP}$. We take advantage of the additive and multiplicative properties of polynomial-based secret sharing schemes to achieve delegation for zk-SNARK**.** Our delegable zk-SNARK achieves $2t+1$ -completeness, $t$-knowledge soundness and $t$-perfect zero-knowledge.