Since privacy of users shouldn't be compromised for solving purposes, we need a way of performing private solving. MPC offers a potential solution to this with guarantees relying on cryptography. I investigated how we can do this during my internship. I wanted to collect some of related discussion and ideas I had about private solving using MPC in a report. The report is available here. It didn't receive any reviews. Any feedback or further ideas are welcome.

Some of related discussion started in theforum discussion. I ended up focusing hash function choice of Taiga. I compared Poseidon and another hash function Hydra for their MPC and ZK efficiencies. It is now available as an ART report.