I remember months ago @JustinDrake was looking into Verifiable delay functions after or around the time of the RANDAO manipulability analysis. What was the outcome of that research? (There are no search results in this site.) Skimming the spec again, I see it mentions related stuff like slashing for early reveals and hardening for orphaned reveals. I skimmed https://eprint.iacr.org/2018/601.pdf, a VDF that doesn't require a trusted setup in an optimal, performant way could use "the class group of an imaginary quadratic order [20], which is an efficient group of unknown order with a public setup [50]." (p. 22, section 7)