Luca de Feo and I wrote up a discussion of isogenies VDFs inhttps://eprint.iacr.org/2020/638

One almost never builds protocols using time-lock puzzles because time-lock puzzles encode only one participant's contribution, making individual puzzles almost worthless. And time-lock puzzles are expensive of course.

We observe that arbitrarily many participants can encrypt messages to the result of one isogeny VDF run. It's basically IBE with the VDF being the private key generator. This radically simplifies advanced voting schemes.

We've one big caveat that you cannot end and restart the isogeny sequence repeatedly, like an isogeny VDF should normally do. As a result, delay encryption requires terabytes of VDF parameters, where an isogeny VDF alone admits a flexible parameters size. It's extremely expensive equip delay encryption evaluators with several terabytes RAM of course, but one might reduce this with enough SSDs in parallel.

Isogeny VDFs require a trusted setup, but a painless one, nothing like the RSA nastiness. You generate the VDF parameters after the trusted setup, so the trusted setup itself remains tiny.

I'd hoped the large VDF parameters might yield memory bandwidth hardness. I'm afraid this appears far from applicable, but one might achieve some limited memory bandwidth hardness for commodity CPUs with a 20x improvement in isogeny evaluation time from the theory side. I still suspect isogenies VDFs can provide higher confidence than other VDF designs, but they require more work and look more expensive per evaluator.

We did not explore if/when physics might impose limits upon piping in those isogeny parameters. We did not explore if residue number systems for known fixed fields yields higher confidence in VDF performance than residue number systems for RSA moduli or class groups. Isogenies VDFs have interesting variants that merge isogeny sequence with multiple start times, which we did not explore either.