At Skale we are looking to implement threshold encryption based on Elliptic curve pairing.

Usually threshold encryption is using symmetric pairing G1 x G1 -> G2

We are looking to modify it to use asymetric pairing used in ETH precompiles

G1 x G2 -> GT

I wonder if anyone here is familiar with the subject …

Usually threshold encryption is using symmetric pairing G1 x G1 -> G2

We are looking to modify it to use asymetric pairing used in ETH precompiles

G1 x G2 -> GT

I wonder if anyone here is familiar with the subject …