At Skale, we need to do threshold encryption in our PoS chains in order to provide protections against front running (essentially a transaction is submitted to the chain in encrypted form, and then decrypted after it has been committed.

We already have BLS signatures implemented in a way compatible to precompiles from ETH 1.0. I am looking for a spec to implement threshold encrypt/decrypt using the same primitives and pairing used in BLS signatures.