2020-02-05 Meeting Notes

1. Question about single secret leader elections, paper from Dan Boneh and others.
    a. https://eprint.iacr.org/2020/025.pdf
2. Short Dynamic Threshold Group Signatures–paper discussion
    a. https://eprint.iacr.org/2020/016.pdf
3. Discussion of key exchange for Indy and Aries
4. Generic Shamir secret sharing protocol:
    a. Mostly just private keys: credential issuers, BBS+ signatures, generally field elements.
    b. Can reveal private key in process of combination? Seems yes.
5. Discussion of block ciphers with nonce reuse resistance properties.
    a. https://eprint.iacr.org/2020/067.pdf