2019-07-24 Meeting Notes

1. Discussion of RFC for Cramer-Shoup verifiable encryption.
   a. RFC could use more motivation on why we need it (Indy will use it).
   b. Generally well-written and well-done by Lovesh.
   c. Please follow-up and review yourself!
2. Discussion of PKCS#11 led by Jon and Rebecca.
   a. Still more work needs to be done.
   b. We discussed the process: going to merge previous work done by Jon and Rebecca.
3. Potentially more basic interfaces for Ursa: led by Lovesh.
   a. Password hashing, HMAC, etc.
   b. Dan: good and bad reasons to wrap things (multiple implementations are a good reason).
   c. We need an RFC–TODO for Mike, Lovesh, Hart
4. Discussion of Jon's slides for Ursa meetup next week.
   a. Good slides.
   b. Spurred some discussion on what we want Ursa to look like in the future.