2020-04-29 Meeting Notes

1. Zcash has come out with some faster pairing curve libraries in the past week. Now their libraries are much faster than ours, so we should use theirs in our code.
    a. General consensus between Mike, Brent, and Hart
    b. Their libraries are also very well-vetted, so this is also good from a security perspective.
2. Mattr has a node.js implementation of BBS+ for node.js that they will be contributing.
    a. This could potentially lead to a well-maintained version of Zmix in node.js.
3. Discussion on integer encoding.
4. Discussion on verifiable encryption
    a. Signal: https://eprint.iacr.org/2019/1416.pdf
    b. Older, public key: https://www.iacr.org/archive/asiacrypt2011/70730088/70730088.pdf
5. Faster delegatable credentials.