We suggest the use of an adaptation of the Bayer-Groth permutation argumenthere to obtain a secret single-leader election with low prover overhead. (Related post here.)

Construction

Let g

be an elliptic curve generator. Let v_1, ...,v_k

be a list of validators to secretly shuffle for block proposals. Every validator v_i

has a permanent public key pk_i

as part of their validator record where pk_i=g^{sk_i}

for some secret key sk_i

. To begin an ephemeral base is set to epk = g

.

To shuffle a set of ciphertexts participate in the election a validator v

broadcasts:

- a new ephemeral base epk' = epk^r
- shuffled public keys pk_1', ... , pk_k'
- a corresponding SNARK proof \pi

with public inputs pk_1,...,pk_k, epk

and private inputs (r, \sigma )

such that pk_i'=pk_{\sigma(i)}^{r}

and epk'=epk^r

A participant can identify their public key as the value pk_j'

such that pk_j' = (epk')^{sk_i}

. If the shuffle is accepted, then the ephemeral base is updated to epk' = epk

and the public keys are updated to (pk_1, ... , pk_k) = (pk_1', ... , pk_k')

.

To limit the damage of a dishonest shuffler, it will be necessary to commit to the shuffle \sigma

in advance of knowing the current ordering of public keys.

Motivation

Justin Drake proposed a low overhead secret single leader election. However, for security, his idea required the use of a private broadcast mechanism (e.g. Tor). Recently Dan Boneh, Saba Eskandarian, Lucjan Hanzlik, and Nicola Greco proposed a means to remove the private broadcast mechanism by instead encrypting the shuffled ciphertexts here. In this proposal we specify a means to instantiate the zero-knowledge shuffle argument.

For more technical detail seehere