For background see Minimal anti-collusion infrastructure

One challenge of the MACI design is that the level of privacy it offers is lower

than a simple ZKP based alternative, because whereas in the ZKP model privacy is unconditional, in MACI if the operator is malicious or compromised, privacy is lost. This post proposes a modification, where privacy is preserved unconditionally, and only anti-collusion properties are operator-dependent.

We allow two new types of interaction with the operator:

1. Deactivate a key, and save a commitment H(s + 1)

for some secret s

if this deactivation was successful (ie. the signature is valid and the key was active). The operator maintains the set of commitments.

1. Provide a ZKP that shows that you have the s

value corresponding to any one

of the saved commitments, revealing a “nullifier” H(s + 2)

. If this ZKP is valid and H(s + 2)

was not yet submitted, a key gets added to the active key set representing yourself.

Note that there is a challenge in (2): for the user

to be able to generate a ZKP, the user must have a set of saved commitments, but opening this data up to the user would allow the user to determine currently active keys, which could be used to credibly buy/sell keys. For the operator

to be able to generate a ZKP, the operator must know s

, which would break privacy.

To get around both issues, we instead have a 2-of-2 MPC between the user and the operator generate the ZKP. Neither the user nor the operator find out each other’s private information, and the operator gets the ZKP and the user does not (we accomplish this by having the MPC encrypt the ZKP to the operator’s public key; if the computation fails it encrypts random junk data to the operator’s public key).

This protocol achieves the following properties:

- When performing either interaction (1) or interaction (2), the user does not learn if the interaction succeeded
- If a user does interaction (1) then interaction (2), at the same time as other users do both interactions, the operator does not learn which user has which key

The operator can thus be prevented from learning which initial participant performed which actions, strengthening the scheme’s privacy properties.