TL;DR

We propose the Collusion-Resistant Impartial Selection Protocol (CRISP) to improve on MACI's honest Coordinator assumption. By leveraging threshold cryptography and fully homomorphic encryption (FHE), we enable a distributed set of Coordinators (a "Coordinator Committee") and shift the trust model from an honest Coordinator assumption to an assumption that there is no threshold of dishonest Coordinators in the Coordinator Committee. We propose to increase the trust model further by introducing economic disincentives for compromised Coordinators.

Background

In 2019, @vbuterin proposed Minimal Anti-Collusion Infrastructure (MACI), a mechanism to enable collusion-resistant voting that inherits blockchain's guarantees around correct execution and censorship resistance. MACI has since been implemented by the EF's Privacy & Scaling Explorations team, and later leveraged by clr.fund to enable collusion-resistant quadratic funding (QF).

At a high-level, MACI works as follows:

1. A trusted "Coordinator" creates a cryptographic keypair and publishes the public key.
2. Participants publish their vote onchain as encrypted messages to the Coordinator.
3. The Coordinator privately tallies the votes and publishes the result, along with providing zero-knowledge proof that the published tally is the result of the messages published on chain.

MACI gains strong cryptographic guarantees of correct execution from its use of zero-knowledge proofs to validate that the output provided by the Coordinator could only have been computed using the inputs published onchain. As such, the Coordinator cannot arbitrarily change or censor votes. However, MACI's privacy and collusion-resistant properties are dependent on the honesty of the Coordinator. The Coordinator can decrypt all inputs (see the plaintext for all votes), meaning a malicious or compromised Coordinator can exert collusive influence over the result.

Proposed Solution

In his original post on MACI, @vbuterin suggests the following future work:

Minimal anti-collusion infrastructure

See if there are ways to turn the trust guarantee for collusion resistance into an M of N guarantee

We propose the Collusion-Resistant Impartial Selection Protocol (CRISP) as an incremental improvement to MACI, increasing the privacy and collusion-resistance guarantees from an honest Coordinator assumption to an assumption that there is no M/N dishonest Coordinators. Further, we propose to introduce economic guarantees for good behaviour by including slashing conditions for Coordinators who provably misbehave.

At a high-level, we propose that CRISP could work as follows:

1. A set of Coordinators are selected (perhaps via sortition from a pool of available Coordinators), along with a specified threshold, to form a Coordinator Committee.
2. Using threshold cryptography, the Coordinator Committee creates and publishes a shared public key, which requires a threshold of the committee members to provide a signature to produce a message signed by, or to decrypt data encrypted to, their shared public key.
3. Participants publish their votes onchain as encrypted messages to the Coordinator Committee's shared public key.
4. Using fully homomorphic encryption (FHE), anyone can run a computation over the published vote ciphertexts to produce the ciphertext of the final tally results. The computation can be executed in a provable environment, like the RISC Zero VM or Arbitrum's WAVM, ensuring the ciphertext output is provably the result of the published votes.
5. A threshold of the Coordinator Nodes can then collectively decrypt the ciphertext output. Revealing the outcome of the vote, without revealing any of the inputs or intermediate states.

In this way, CRISP improves the trust assumptions beyond MACI's reliance on an honest Coordinator to an assumption that there is no dishonest threshold in the Coordinator Committee. To further strengthen the trust assumptions, we suggest requiring each individual Coordinator to provide a deposit subject to slashing upon proof that their keys were used for anything beyond setting up the Coordinator Committee's shared key and decrypting the output ciphertext.

Future Work

We are currently working on a proof of concept implementation and will hopefully have more to share in the coming weeks and months. If you're interested in contributing, please reach out!