Original Publication:
https://github.com/rohanrhu/TruthfulMultiplayerRandomness

17 November 2023

Meowing Cat

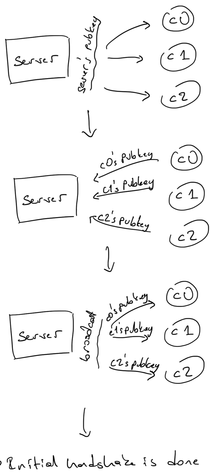
Author: Oğuzhan Eroğlu (https://github.com/rohanrhu)

All of this this things provide a true multiplayer randomness...

Truthful Multiplayer Randomness

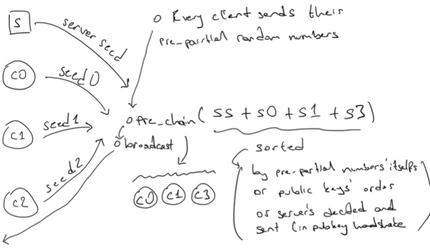
Handshaking

- All clients of the hand and server perform an handshake

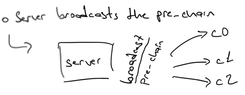


- Partial handshake is done

Building Pre-chain



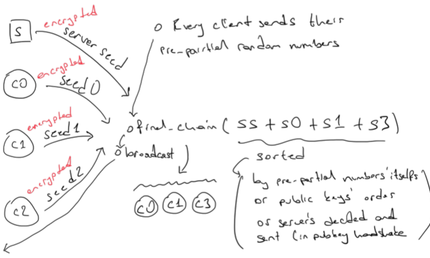
- Server broadcasts the pre-chain



- Now all players have the pre-chain

Building final chain

- Every player sends final-partial random numbers which is encrypted version of pre-partial random numbers by that player's private key



Verifying final chain

- Every client checks the final chain by verifying every player's partial random numbers by their handshaked public keys for that if they are encrypted with that player's private keys by decrypting the final-partial random number of that player with that player's public key
- The true randomness is provided by the fact that every player has their own partial random number too in the chain

Deriving App-specific Random Number

- The app that implements Meowing Cat's Truthful multiplayer Randomness reduces/derives the app-specific derivation of the final random chain with a method like modular arithmetic or hashing algorithm or another reducer function

Players Know Who They Are Playing With

- Every player (client) can create new random pubkey/privkey pairs anytime
- Players shares/exchanges their public keys between themselves in any communication way

Every player/client can add public keys with a label and they can make sure that they are playing with that players