Mixing

Each server in the mix-net perform the same actions during execution.

1. It is given the list of ciphertexts from the previous server.
2. It reencrypts these ciphertexts with its private key.
3. It randomly shuffles the list of ciphertexts.
4. It passes the reencrypted and shuffled list of ciphertexts to the next server.

During these steps a zero-knowledge proof is produced which can prove that the server indeed did output a list of shuffled and reencrypted ciphertexts without tampering with the ciphertexts.