Private Tor Statistics

We rely on:

- A set of authorities
- A homomorphic public-key scheme (AH-ECC)
- Count-Sketch (a variant of CMS)

Setup phase

- Each authority generates their public and private key
- A group public key is computed

Private Tor Statistics

Each HSDir (router) builds a Count-Sketch, inserts its values, encrypts it, sends it to a set of authorities

The authorities:

- Add the encrypted sketches element-wise to generate one sketch characterizing the overall network traffic
- Execute a divide and conquer algorithm on this sketch to estimate the median