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

How we do it

The range of the possible values is known

On each iteration, the range is halved and the sum of all the elements on each half is computed

Depending on which half the median falls in, the range is updated and again halved, process stops once the range is a single element

Output privacy:

- Volume of reported values within each step is leaked
- Provide *differential privacy* by adding Laplacian noise to each intermediate value