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

Evaluation

Experimental setup:

- 1200 samples from a mixture distribution
- Range of values in [0,1000]

Performance evaluation:

- Python implementation (*petlib*)
- 1 ms to encrypt a sketch (of size 165) for each HSDir and 1.5 sec to aggregate 1200 sketches