

Communication Analysis

Aim

- Find a network speed at which the number of evaluations per second of our OPRF surpasses the DDH-based libsodium.
- Why would it matter:
 - Currently, DDH based OPRF(libsodium) eval/sec is way lower than our OPRF, but the total number of bits communicated is lower too.
 - The following table shows the difference.

Protocol	Eval/sec	Total Communication	Communication/second
OPRF construction 1	105K	1152 bits	120Mbps
DDH based OPRF (libsodium)	11K	512 bits	5.6Mbps

Point to remember

- A point to note, even though the network bandwidth can be increased beyond 5.6 Mbps, due to computational complexity, DDH-based OPRF can only communicate 5.6 Megabit per second.
- Using this information, we can try to find out the network speed where evaluation/sec of our OPRF surpasses DDH-based OPRF.

Solution

$$\frac{x \text{ Mbps}}{1152 \text{ bits}} > \frac{5.6 \text{ Mbps}}{512 \text{ bits}}$$

$$x \text{ Mbps} > \frac{5.6 \text{ Mbps} * 1152 \text{ bits}}{512 \text{ bits}}$$

$$x \text{ Mbps} > 12.6 \text{ Mbps}$$

- At 12.6 Mbps, the eval/sec for our OPRF is equal to DDH-based OPRF(libsodium).
- Any increase in network bandwidth over 12.6 Mbps will not make DDH-based OPRF any faster as it has already been hit with its computational bottleneck.