Privacy Engineering

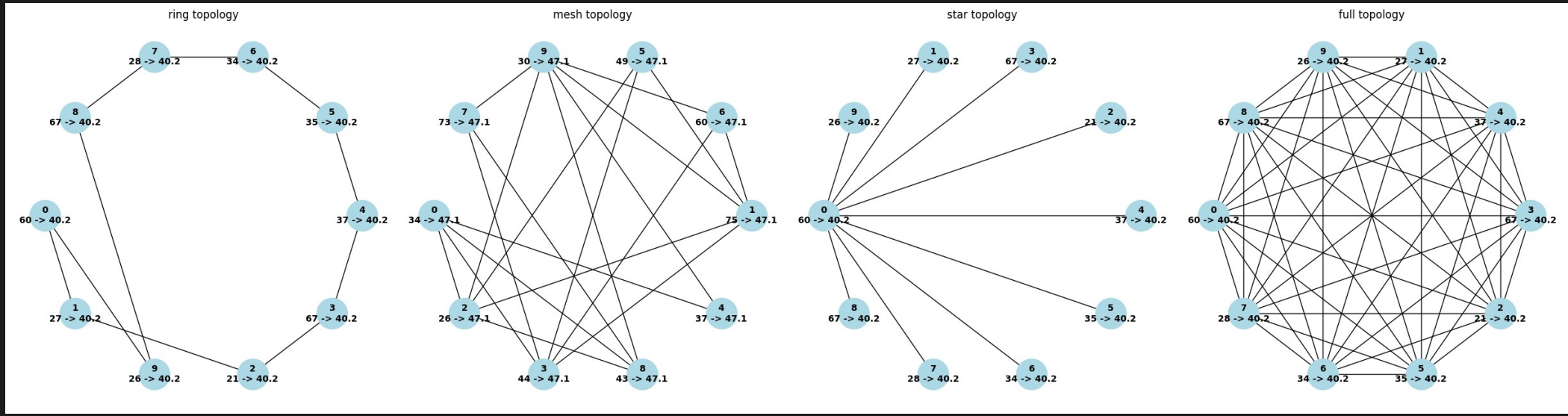
Additive Secret Sharing-based Distributed Average Consensus

Morten Munk Andersen

2026 SW9
20212638

Introduction

- Goal
  - Compute average age of all nodes
  - Don’t reveal individual values



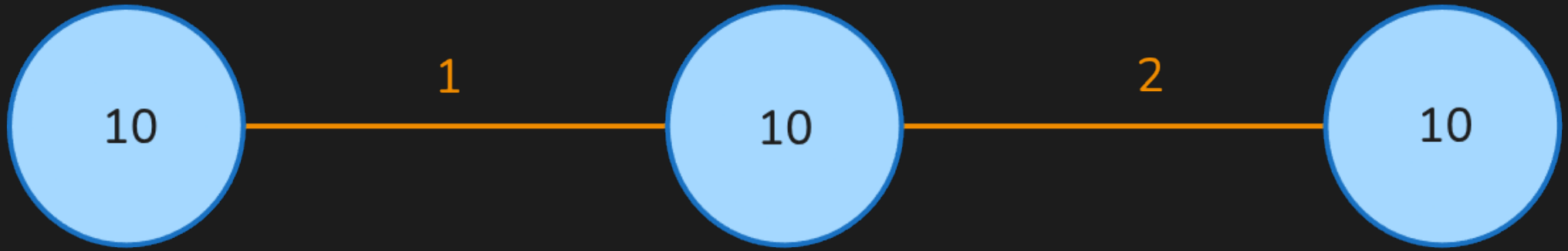
How does it work?

Traditional consensus:

- Neighbors can spy!

This method:

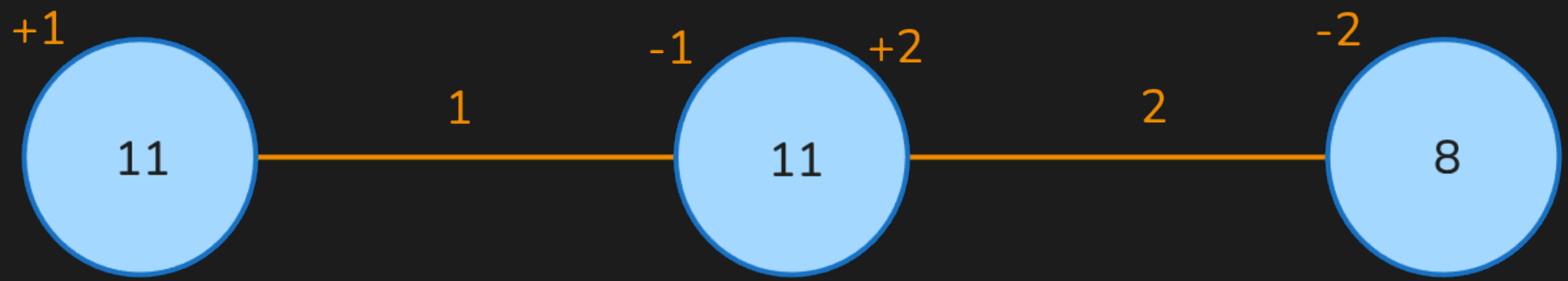
- At least one honest neighbor for it to work!



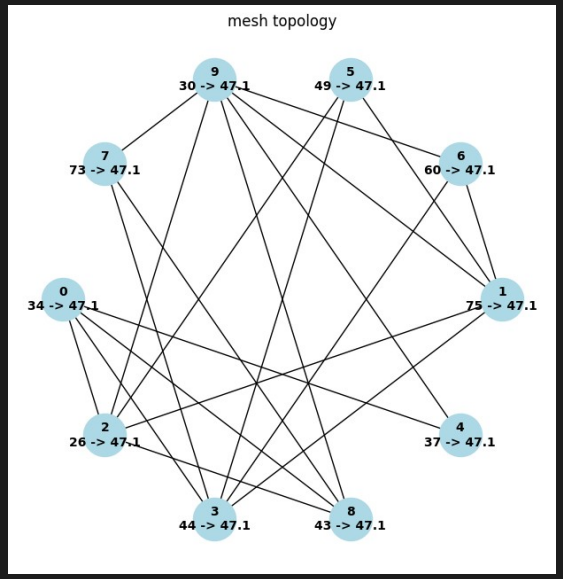
How does it work?

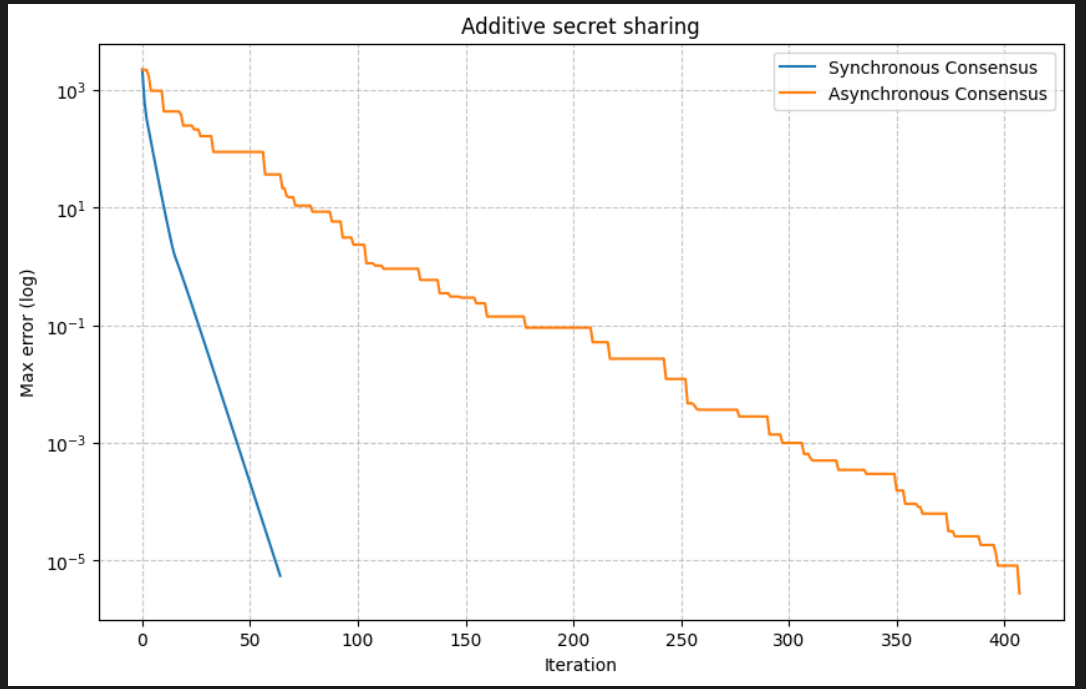
How does it work?

Zero sum mask!



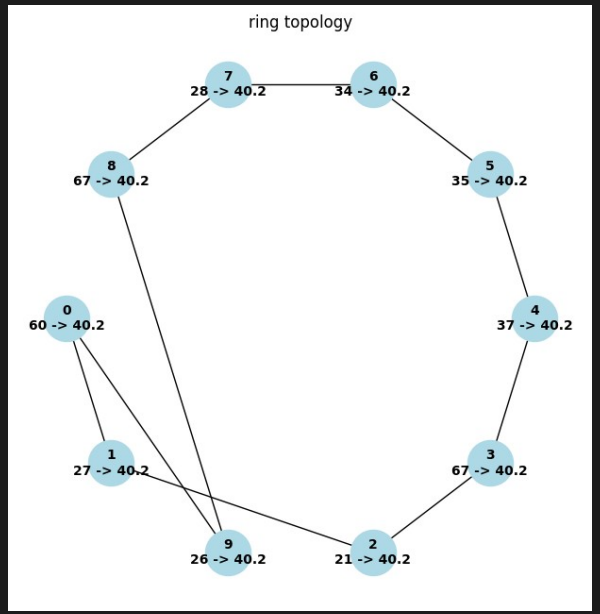
- Sync
  - Global discrete time updates
  - Laplacian weight matrix
- Async:
  - two nodes at a time

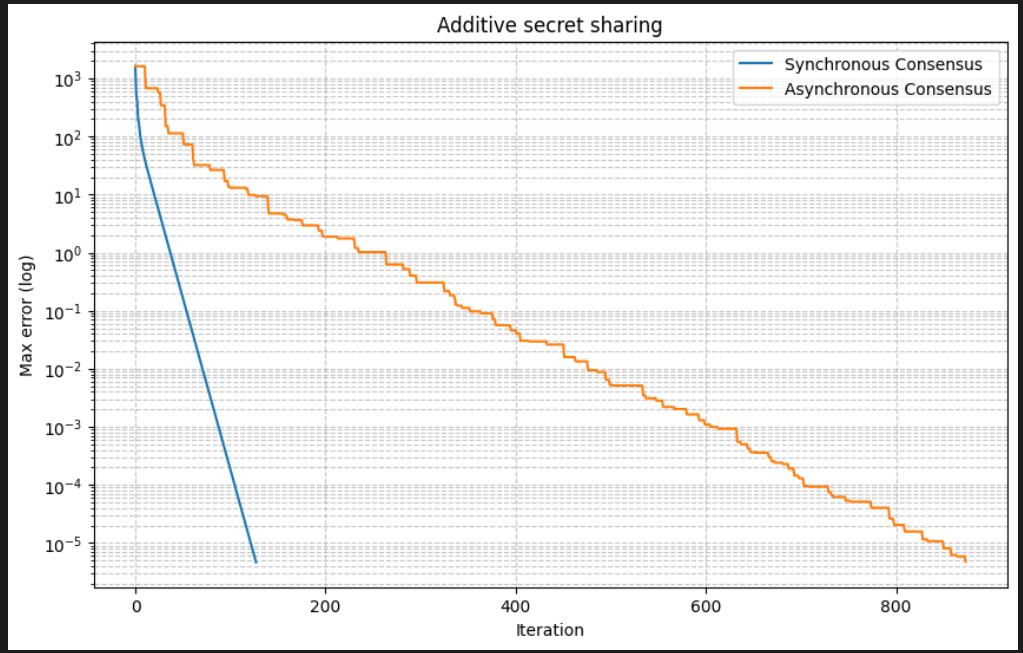




Ring topology

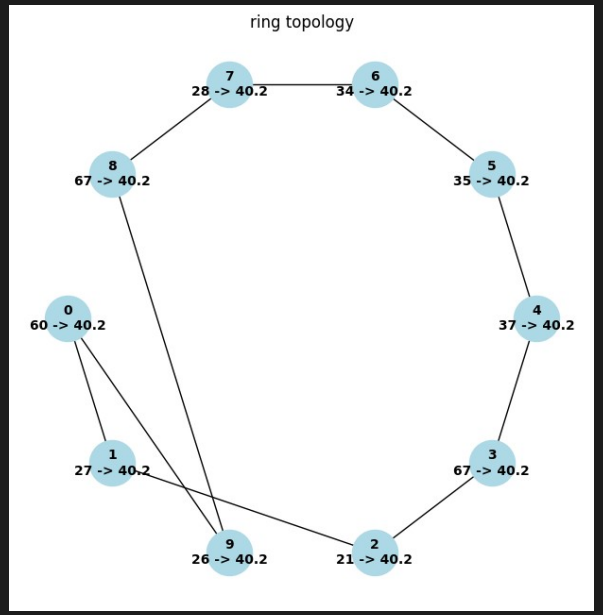
- Potential for wasted iterations in async
  - e.g. two nodes with similar values

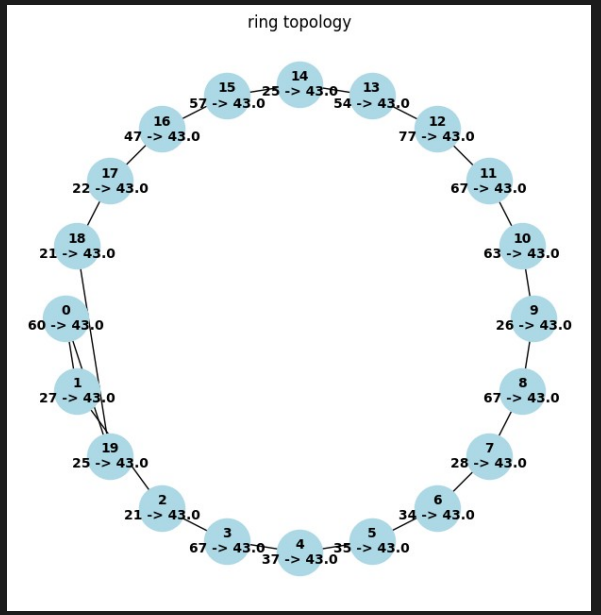




Ring topology

What about more nodes? (10 vs 20)

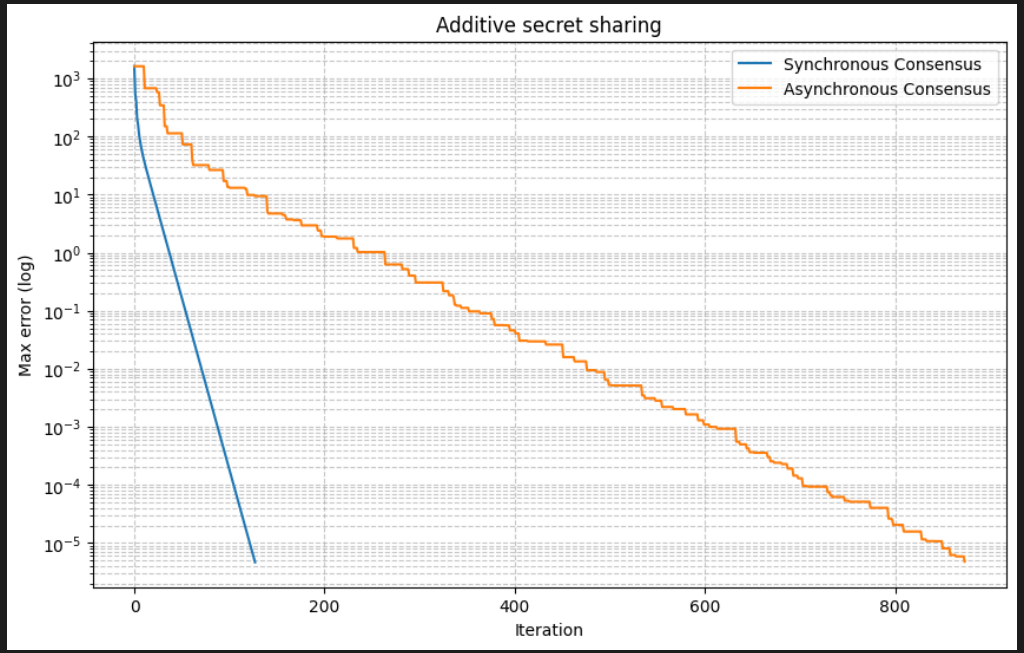


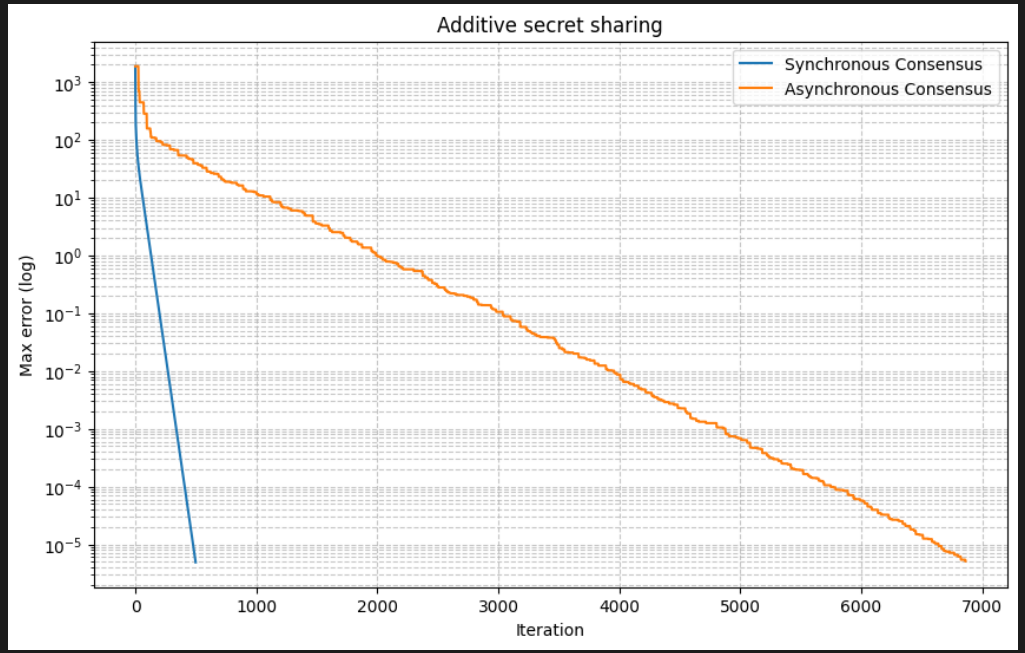


Ring topology

What about more nodes? (10 vs 20)

- Iterations increase

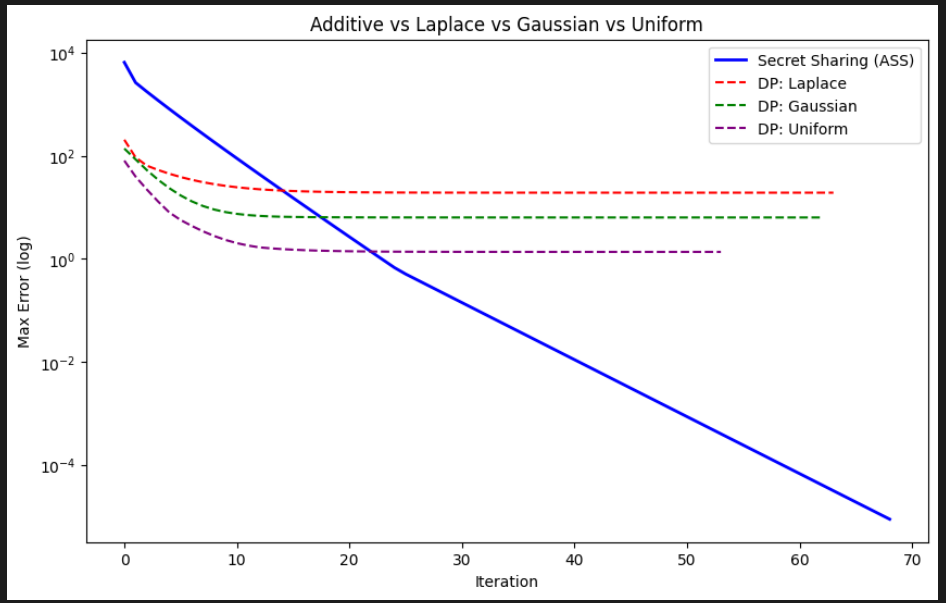




Differential Privacy

Example with mesh (50 nodes)

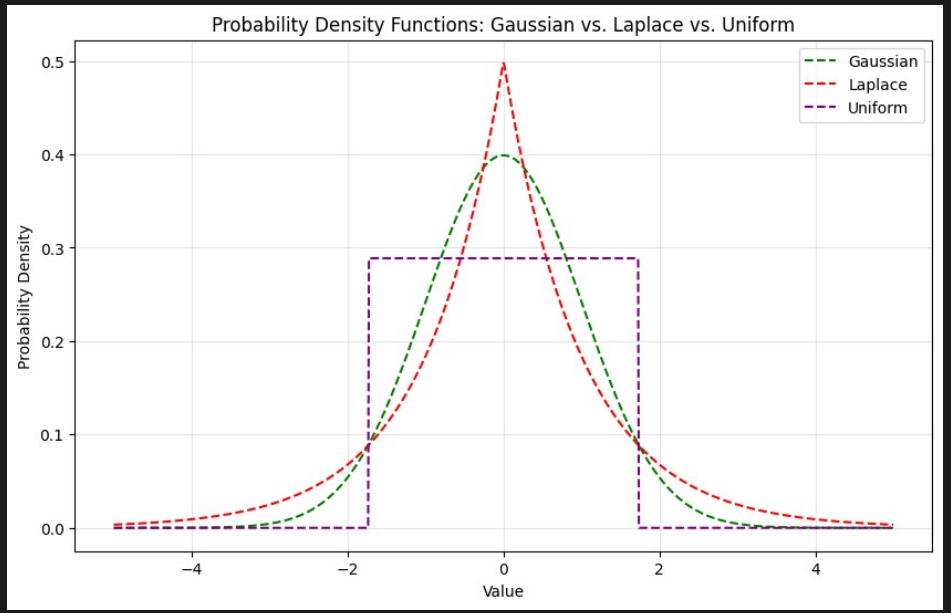
- Additive: zero sum mask
- DP: permanent noise

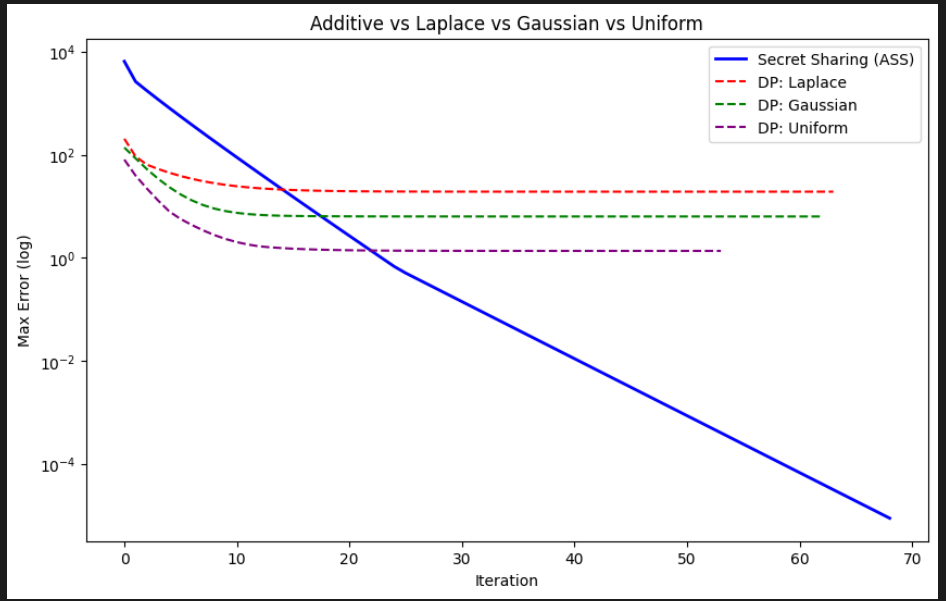


Differential Privacy

ε: The privacy budget (privacy vs accuracy)

δ: Probability of privacy failure

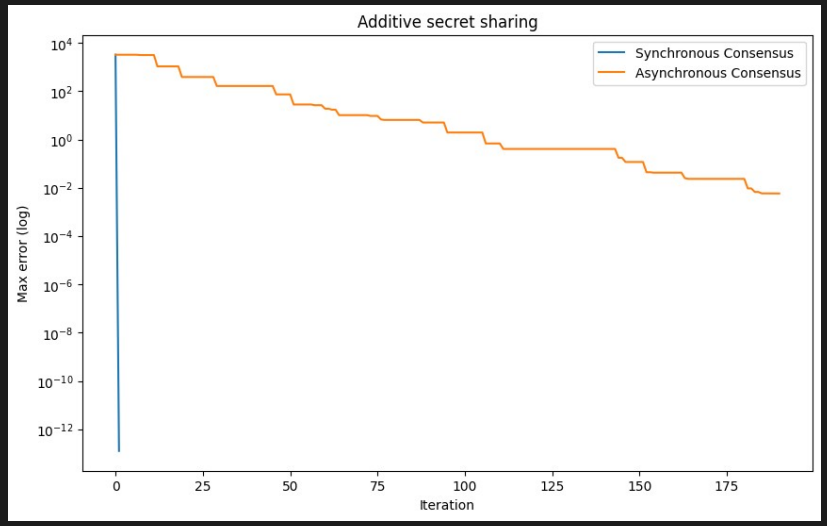




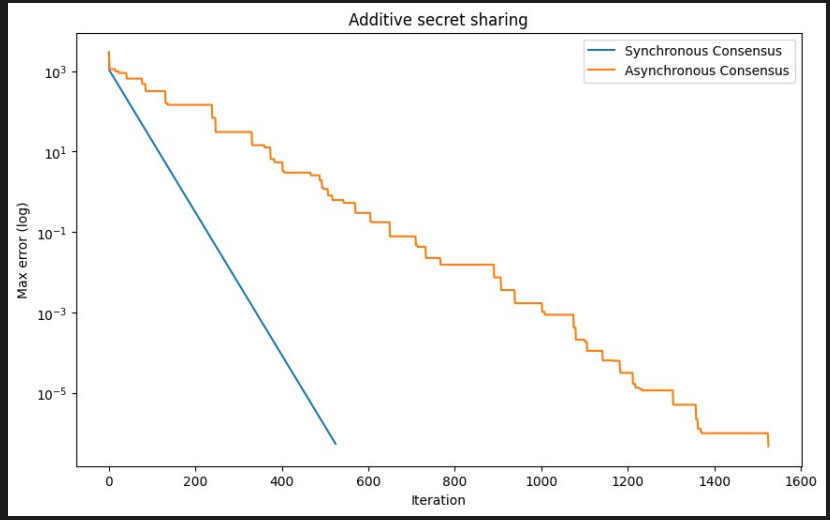
Summary

- Additive Secret Sharing:
  - Neighbors can’t peak at shared values!
- Differential Privacy
  - Combat statistical attacks on final result

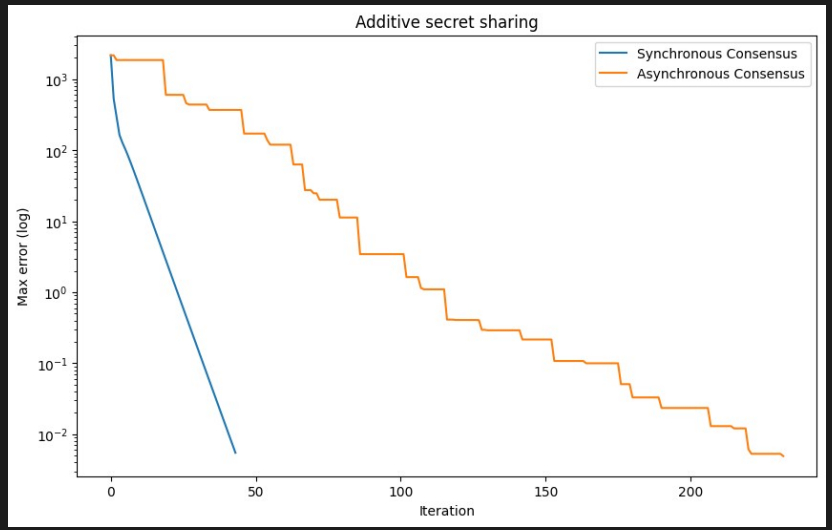
Full



Star



Mesh



Ring