Efficiency considerations

MLS IETF 103

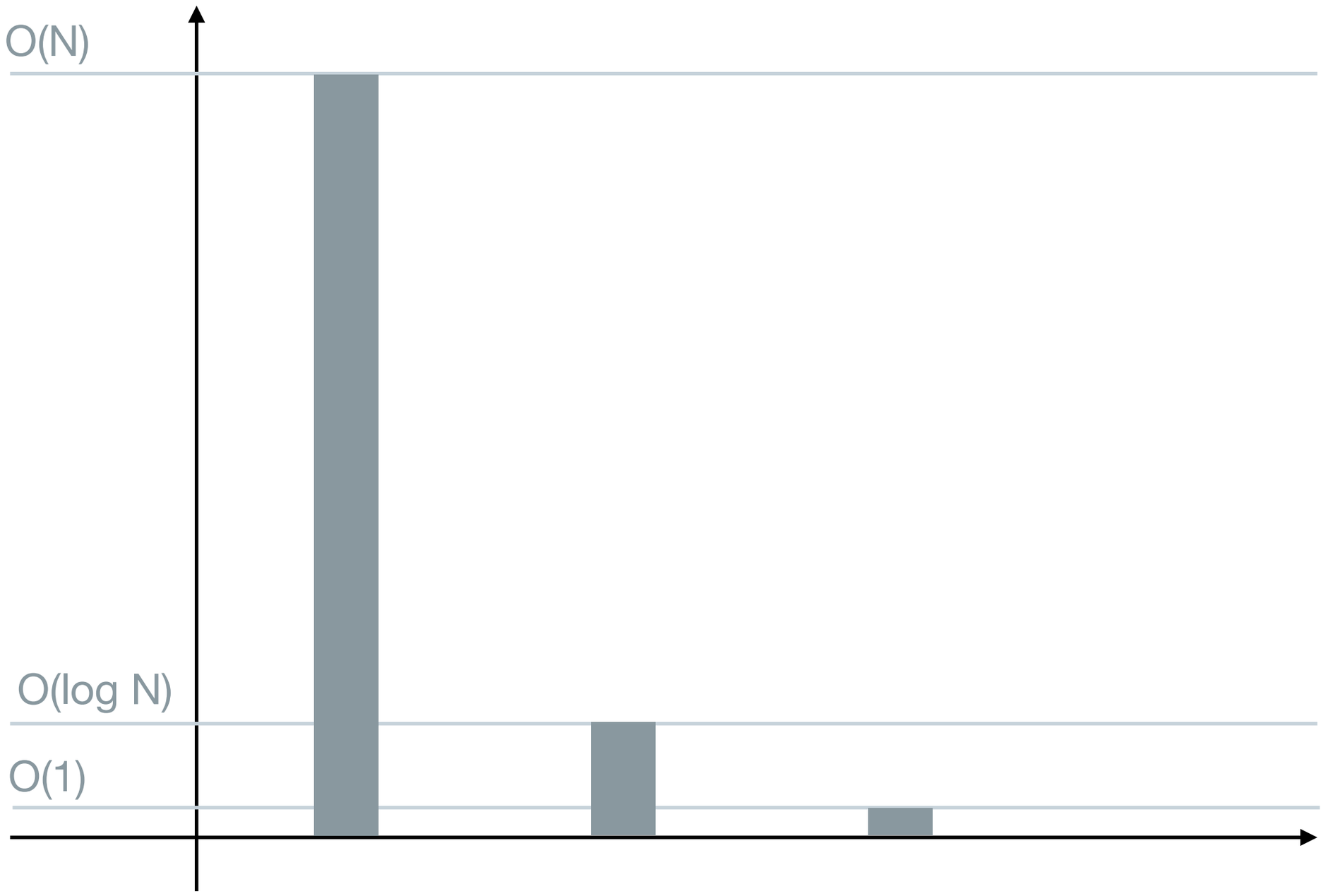
MLS

- Make secure messaging efficient for large groups (50k has been mentioned repeatedly)

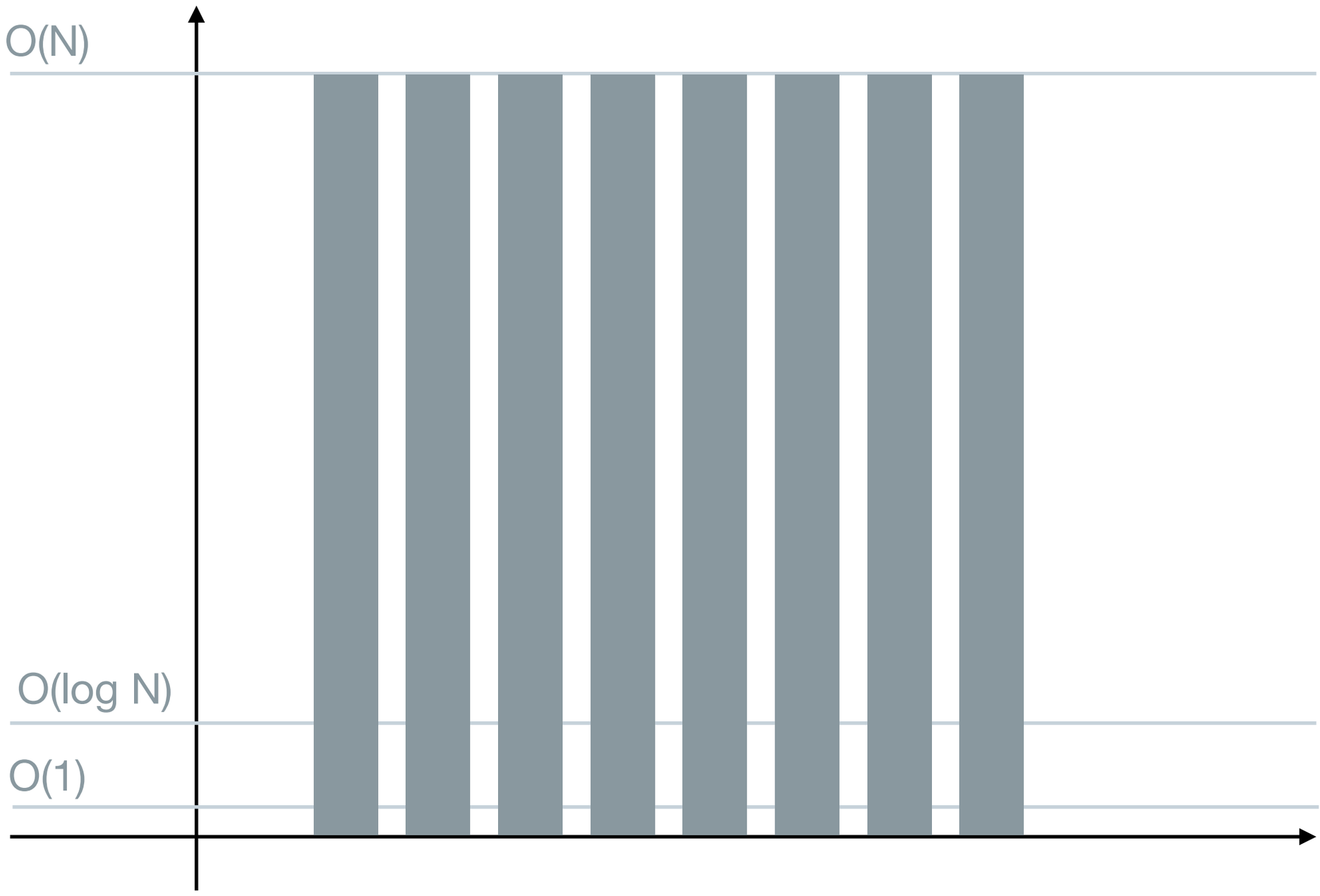
- Improve security guarantees (FS, PCS group membership), compared to existing protocols

- Make it a standard

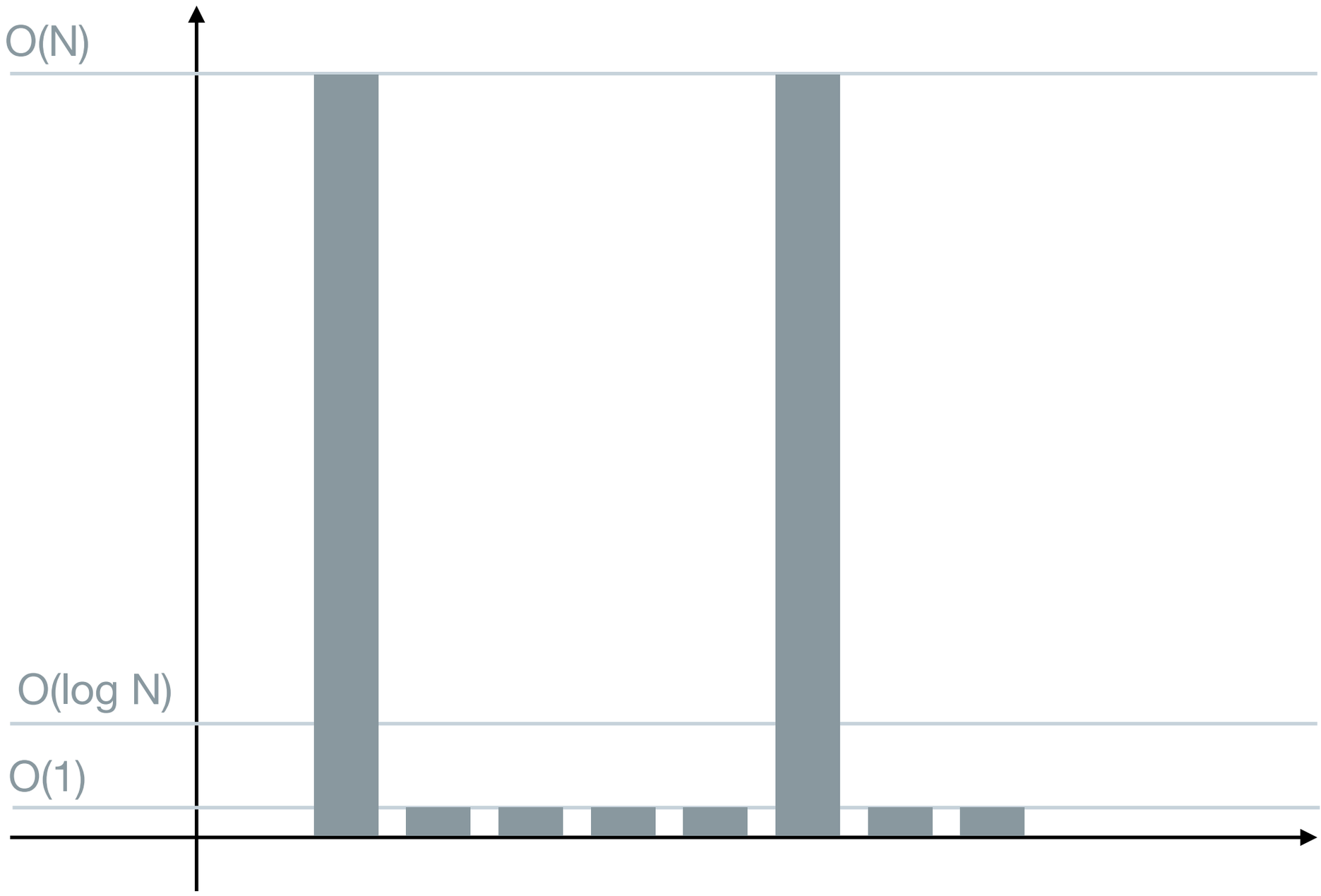
Cost



Cost
Sending messages



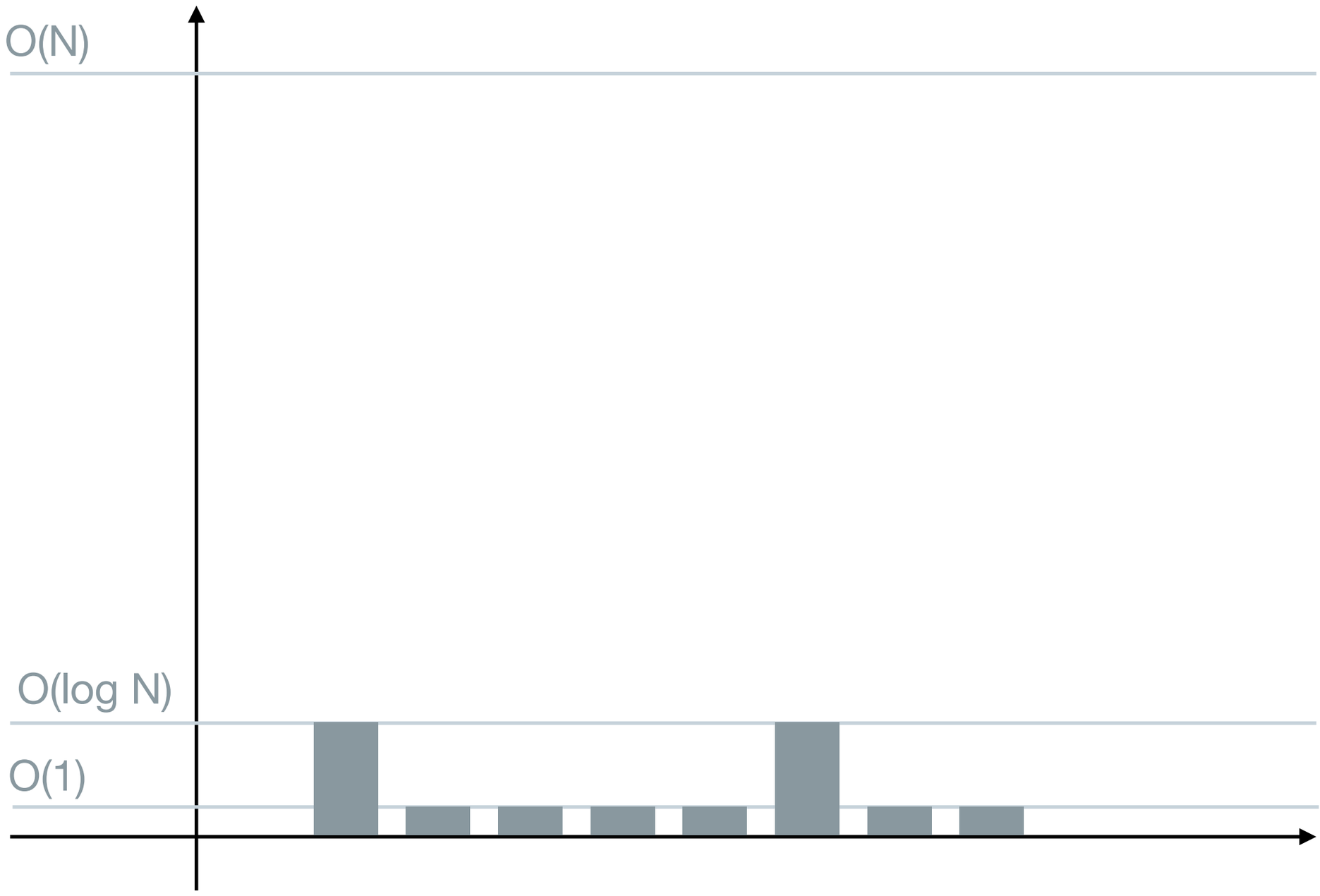
Cost
Group key



Efficiency

- **Definition**: costly operations should at least be in O(log N)

Cost
Ideal situation



Linear cost

- Group creation: Linear but can be reduced to log(N) with warm-up
- Inviting a member: linear cost
- Adding a device: linear cost (with a factor c)

Linear cost

Group size	Size of Welcome HS
100	10 KB
1k	98 KB
10k	980 KB
50k	4.9 MB
100k	9.8 MB

Potential solutions

- Reduce the size of the Welcome message by sending the tree/roster out-of-band

- Server could assist with storing the tree