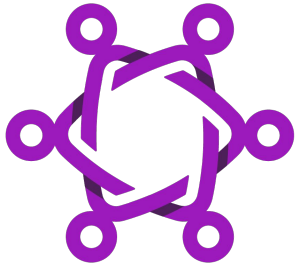


Light Clients

draft-kiefer-mls-light

Problem: Download and Memory

MLS requires that clients download, validate, and store the group's ratchet tree

Each participant only uses one MLSCiphertext in a Commit

… but has to download O(N) data to verify the Commit signature

In large groups, these objects can be L A R G E

In a 1,000-participant Webex meeting (empty tree):

Tree: 3.5MB in memory / 2.3MB gzip'ed

Commit: 391KB

Light Clients

A **light client** is a member of the group that **does not have the ratchet tree**

A light client **cannot commit**

A light client **cannot process a normal Commit**

Instead:

- Light client joins with only a Welcome
- DS transforms Commit into per-light-client LightCommit

A light client can join and follow the group with O(log N) download / memory

Corollaries

Each group must have at least one full (non-light) client

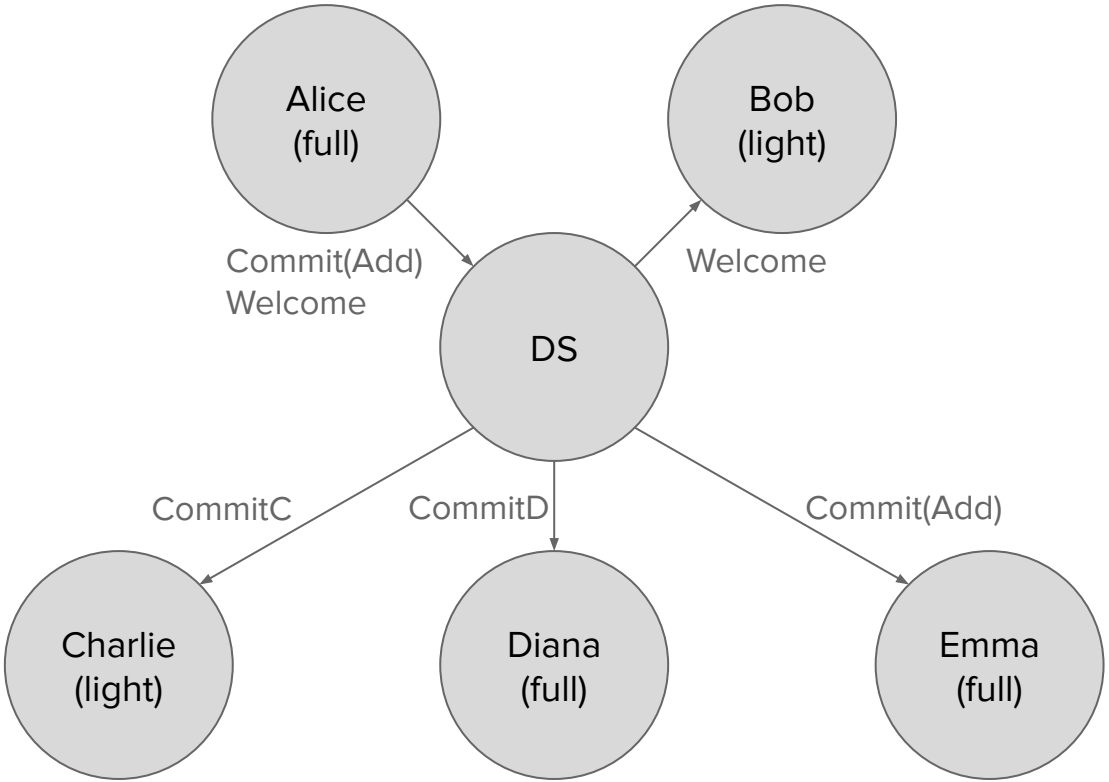
- Someone has to do the commits, otherwise nobody can be added!

Clients can transition between light and full

- Light -> Full: Download and validate the tree
- Full -> Light: Delete local copy of the tree

DS needs to be aware of which clients are light / full

Operating a Group with Light Clients

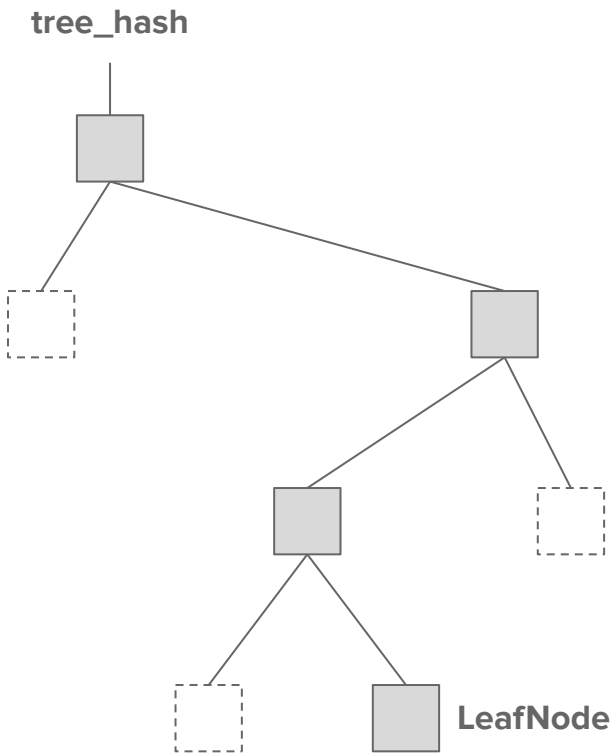


Incremental Authentication

Sometimes a light client wants to authenticate a specific member

- Verify their own membership
- Verify the client that added them
- Verify a specific other client (e.g., active speaker)

Present a “slice” through the ratchet tree – basically a Merkle tree proof chaining to the tree hash



Summary

Ratchet Tree and Commits are heavy in large groups

Light clients can join and follow with O(log N) download and memory

… at the cost of not being able to authenticate the whole group

Three main changes:

Skip the tree validation on join

DS slices Commit into per-client Light Commits

Tree slices allow for authentication of specific other members