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

Sending messages

$O(N)$

$O(\log N)$

$O(1)$
Cost
Group key

\[ O(N) \]

\[ O(\log N) \]

\[ O(1) \]
Efficiency

- **Definition**: costly operations should at least be in $O(\log N)$
Cost
Ideal situation

$O(N)$

$O(\log N)$

$O(1)$
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

<table>
<thead>
<tr>
<th>Group size</th>
<th>Size of Welcome HS</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>10 KB</td>
</tr>
<tr>
<td>1k</td>
<td>98 KB</td>
</tr>
<tr>
<td>10k</td>
<td>980 KB</td>
</tr>
<tr>
<td>50k</td>
<td>4.9 MB</td>
</tr>
<tr>
<td>100k</td>
<td>9.8 MB</td>
</tr>
</tbody>
</table>
Potential solutions

- Reduce the size of the Welcome message by sending the tree/roster out-of-band
- Server could assist with storing the tree