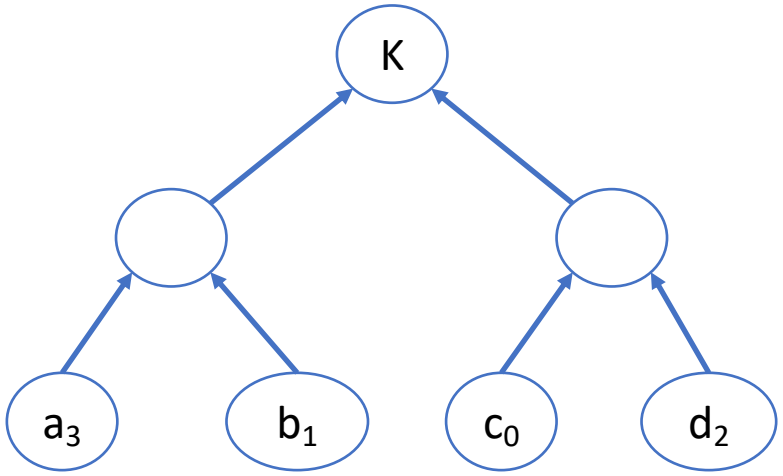
Analysis

status, plans, and missing bits

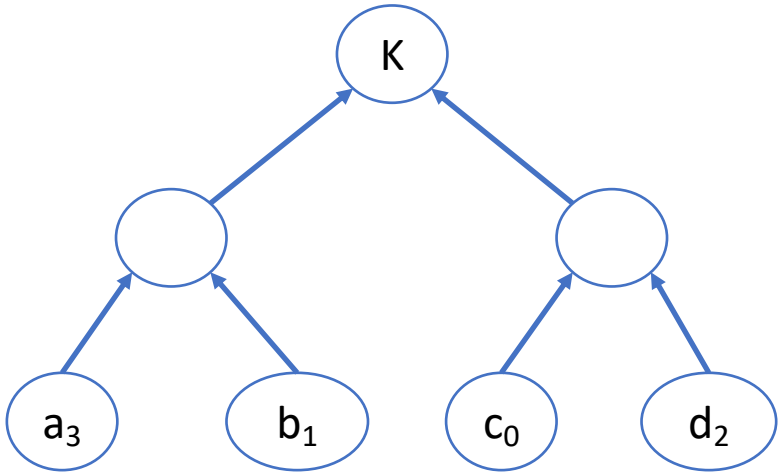
Versioned Members



- Every time a member (?) sends an update, it increases its version number
- The current membership of the group can be seen as a list of versioned members

- *Invariant:* the key K is known only to the versioned members at the leaf

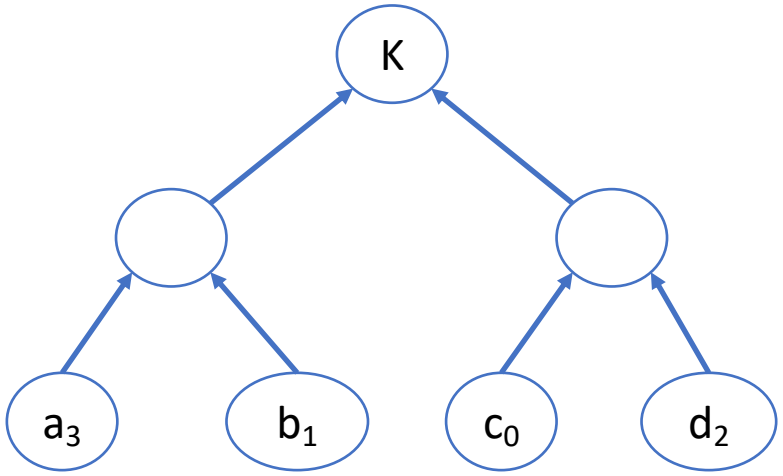
Versioned Members



- *Forward Secrecy:*
  If version 4 of a is compromised, K is still confidential (since a_4 is not in the tree)

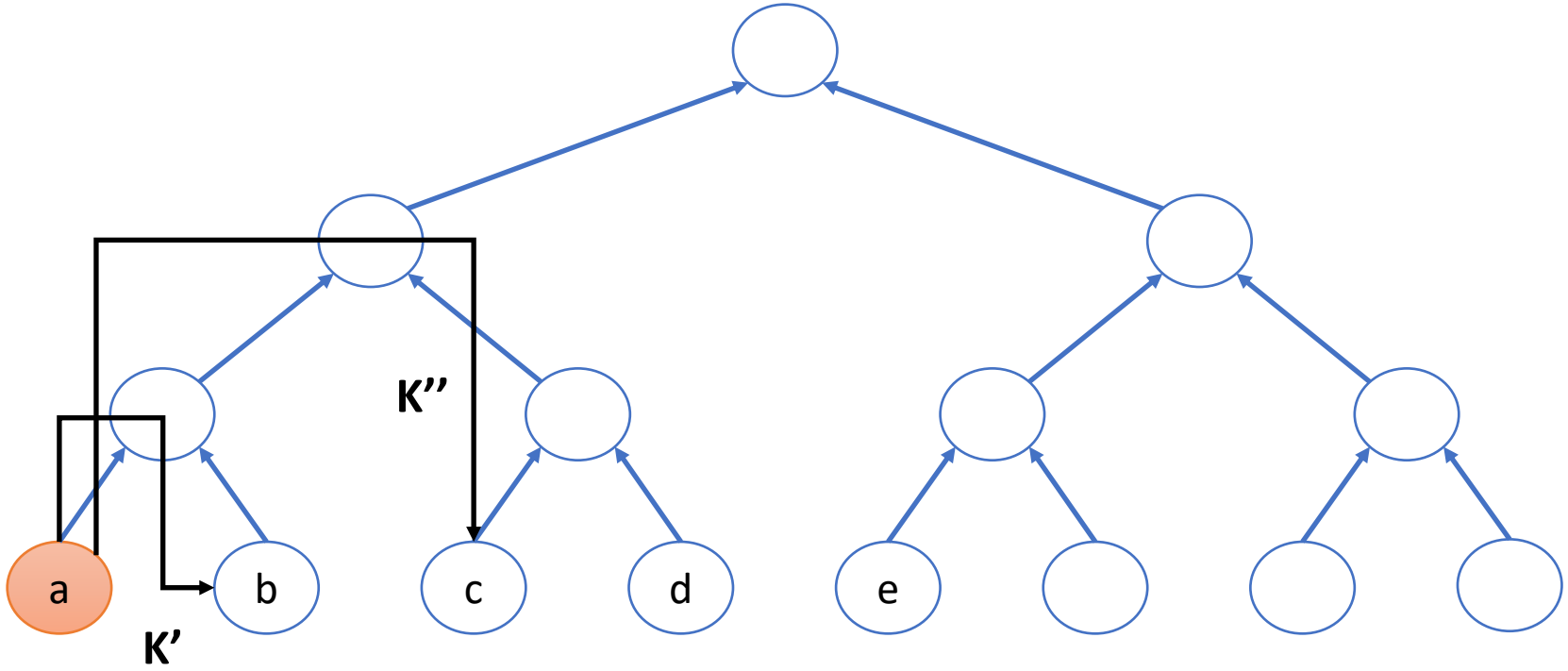
- *Post-Compromise Secrecy:*
  If version 2 of a is compromised, K is still confidential (since a_2 is not in the tree)

Authenticating Versioned Members



- We need each operation to be authenticated by a *versioned* member, i.e. by a_3 (not a)
- *Credentials:*
  Does the authentication service issue credentials for a particular member version?
- *Signature Key Update:*
  If the authentication service provided a credential for version 0, can a member locally generate a credential for version i?

Malicious Members?



Desynchronizing Group State

Prevent malicious participant from creating inconsistent state

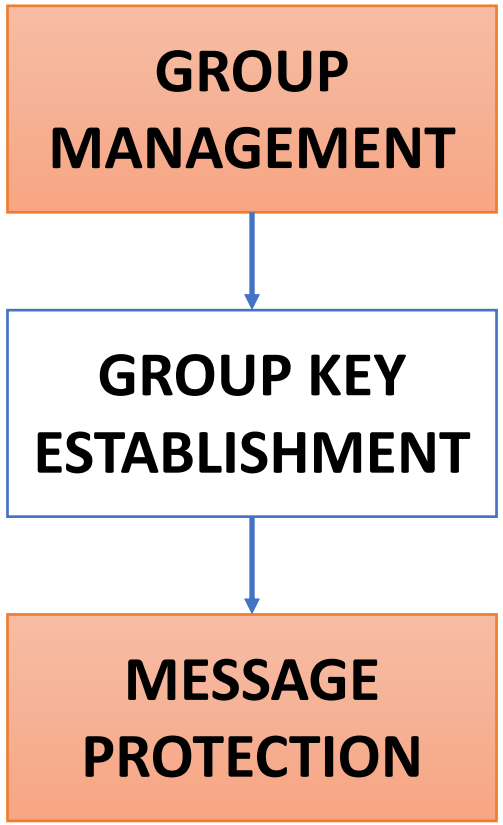
Analysis Status

- Many prior analyses of Signal (symbolic + complexity-theoretic)
- Prior work on ART (https://eprint.iacr.org/2017/666.pdf)

- *Ongoing:* Symbolic security proofs for TreeKEM (ETA: Feb 2019)
- *Ongoing:* Verified F* implementation of TreeKEM (ETA: July 2019)

Other MLS Components (todos)

- Ongoing work (and prior work)



- Who authenticates and how?
- Who authorizes and how?
- Can we reuse keys across groups: signature keys? KEM keys?

- Multiple hash-chains (ongoing)