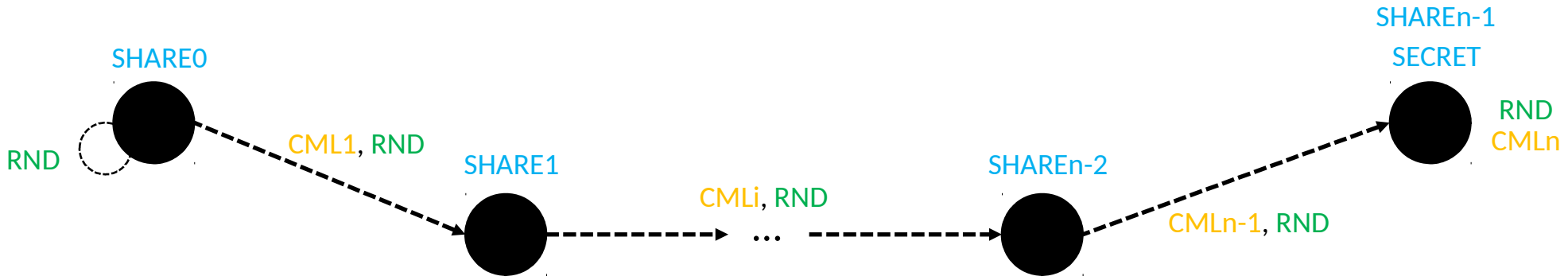
A Proposal for Ordered PoT

Diego R. Lopez, Telefonica I+D

The Goals

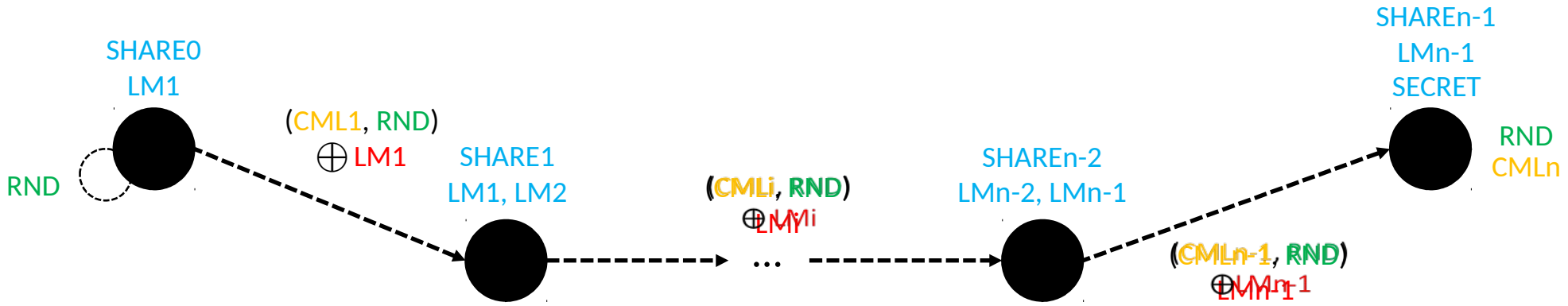
- Support ordered Proof-of-Transit
  - A strong requirement in some cases
- Compatible with current proposal
  - Algorithmically
  - Computationally
  - Operationally
- Built as an extension
  - Support different levels of assurance
- Consider other applications
  - Topology attestation

The Method



Final Check

$CMLn == SECRET + RND$



Final Check

$CMLn == SECRET + RND$

The Next Steps

- Incorporate the changes in the PoT draft
  - Likely, as a new version of section 3.5
  - As recently shared on the list
  - Including any comment this distinguished audience may make
- Update security considerations
  - Some of them already noted
    - Mask management, including refresh
    - Masking operation (XOR vs other choices, including symmetric encryption)
    - Rerouting
  - More inputs extremely welcome