LHIP or Delayed State Setup

- Opportunistic HIP is secure enough (and more) for mobility and multi-homing
  - Vulnerable to MitM during base exchange, but not afterwards
  - Maybe too secure and too costly?
- More lightweight protocols also secure enough for mobility and multi-homing
  - E.g. WIMP, using reverse hash chains
- Maybe we could combine these?

The LHIP idea

- Initially just exchange HITs and WIMP anchors

$H_I i = hash(H_I i+1)$

$H_I 0 = hash(H_I 1)$

- Use WIMP for sole mobility/multi-homing

- Update to full HIP if needed