## 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_{T}0 = hash(H_{T}1)
```

- Use WIMP for sole mobility/multi-homing
- Update to full HIP if needed

```
LI1: \operatorname{HIT}_{I}, \operatorname{HIT}_{R} or \operatorname{NULL}, \operatorname{mac}(\operatorname{H}_{I}^{0})
LR1: HIT<sub>I,R</sub>, puzzle, sig, temp_H<sub>R</sub>0
LI2: HIT<sub>I,R</sub>, solution, H<sub>I</sub>0
LR2: HIT<sub>I,R</sub>, H<sub>R</sub>0
REA: HIT_{I,R}, H_{I}1, locs, mac(H_{I}2)
AC: HIT<sub>I,R</sub>, H<sub>R</sub>1
ACR: HIT<sub>I,R</sub>, H<sub>I</sub>2
I1: HIT<sub>I,R</sub>, H<sub>I</sub>3
R1: \text{HIT}_{I,R}, \text{H}_{R}^{2}, rest of R1
I2: \operatorname{HIT}_{I,R}, \operatorname{H}_{I}4, rest of I2
R2: HIT_{I,R}, H_R3, rest of R2
```