```
i -> (a,6): {Ea(1)}_kab
(a,6) -> i: {{K(2)}_Ea(1)}_kab
i -> (a,3): {{K(2)}_Ea(1)}_kab
(a,3) -> i: {Na(3)}_K(2) witness(a,b,na,Na(3))
i -> (a,6): {Na(3)}_K(2)
(a,6) -> i: {Na(3),Nb(4)}_K(2) witness(a,b,nb,Nb(4))
i -> (a,3): {Na(3),Nb(4)}_K(2)
(a,3) -> i: {Nb(4)}_K(2)  request(a,b,nb,Nb(4))
```

Parallel session attack, man-in-the-middle between A as initiator and A as responder, attacker masquerades as B, but no secret nos are exposed.

HLP Specification

```
ro eke_Init (A,B: agent,
               Kab: symmetric_key,
               Snd,Rcv: channel(dy))
played_by A
def=

  lol State   : nat,
        Ea      : public_key,
        Na,Nb,K : text

  cot sec_k1 : protocol_id

  init  State := 0

  transitio

   1. State = 0
      /\ Rstart)
      =|>
      State' := 1
```