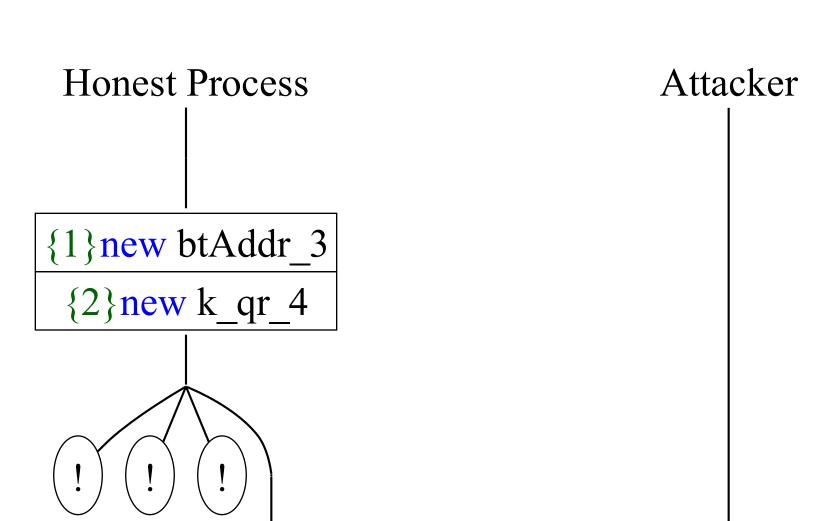
A trace has been found.



Phase 1

$$(\sim M, \sim M_1) = (kw, km)$$

The attacker has the message $\sim M = kw$ in phase 1