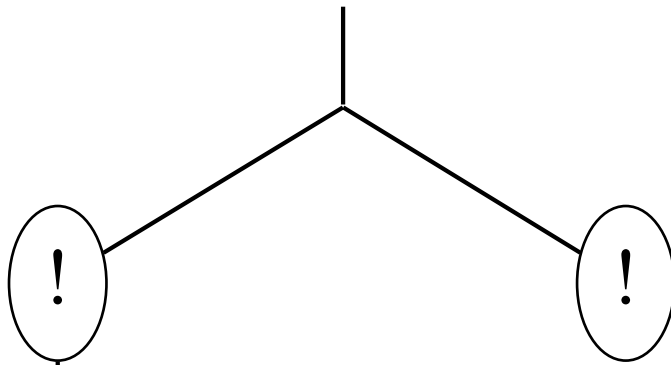


A trace has been found.

Honest Process

Attacker



Beginning of process **sender**

$\sim M = \text{hash}(s)$

{3}event endS



The attacker tests whether
 $\sim M = \text{hash}(@\text{weaksecretcst})$
knowing
 $\sim M = \text{hash}(s)$.
This allows the attacker to know whether $@\text{weaksecretcst}$
= s.