Private 127.0.0.1

Running Tamarin 1.8.0 Index Download Actions » Options »

Proof scripts

Message theory

Multiset rewriting rules (8)

Tactic(s)

Raw sources (10 cases, deconstructions complete)

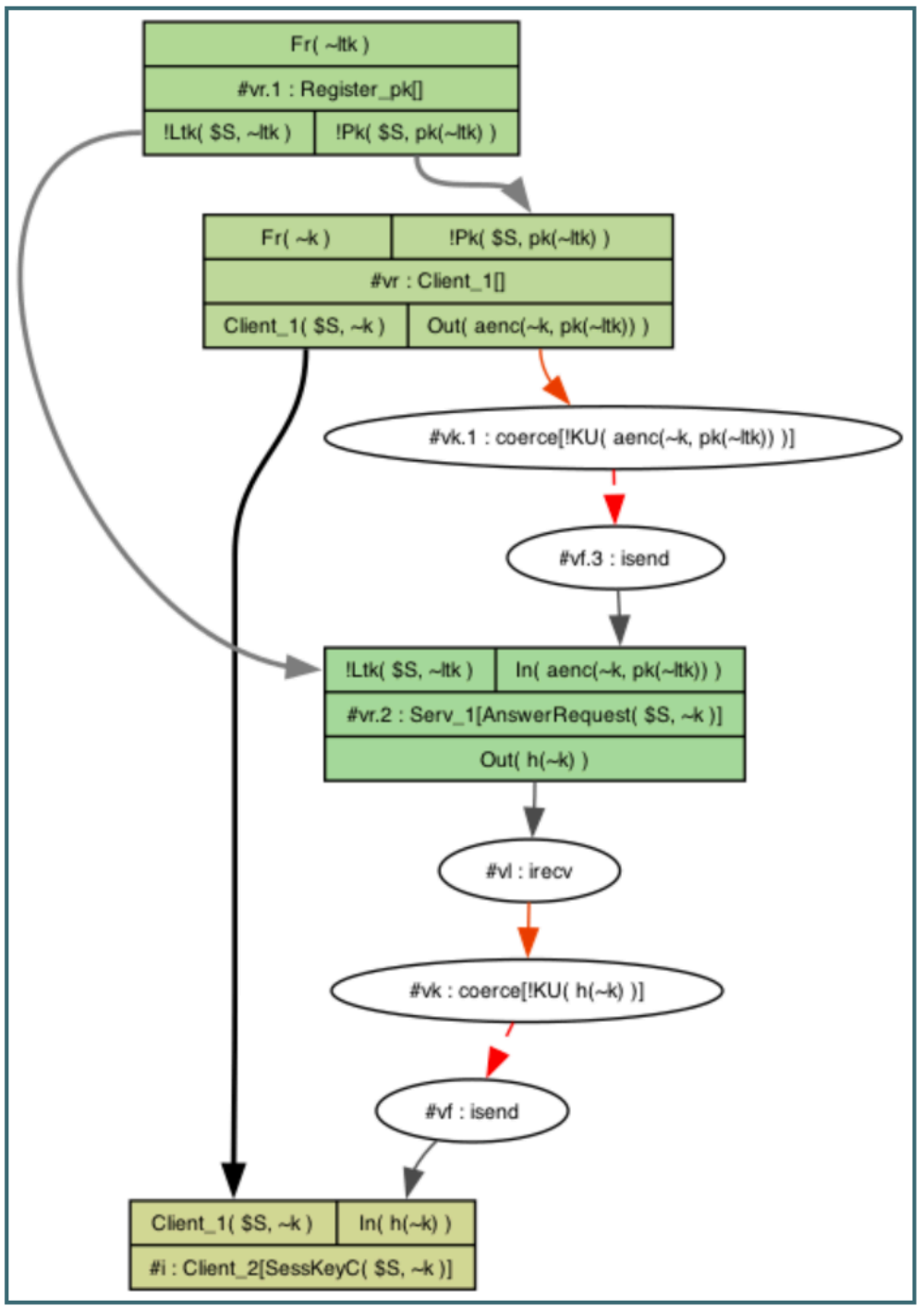
Refined sources (10 cases, deconstructions complet

```
lemma Client_session_key_secrecy:
  all-traces
  "¬(∃ S k #i #j.
          ((SessKeyC( S, k ) @ #i) ∧ (K( k ) @ #j))
          (¬(∃ #r. LtkReveal( S ) @ #r)))"
simplify
solve( Client_1( S, k ) ▶₀ #i )
  case Client_1
  solve( !KU( ~k ) @ #vk.1 )
    case Client_1
    solve( !KU( ~ltk ) @ #vk.2 )
      case Reveal_ltk
      by contradiction /* from formulas */
    qed
  qed
qed

lemma Client_auth:
  all-traces
  "∀ S k #i.
         (SessKeyC( S, k ) @ #i) ⇒
         ((∃ #a. AnswerRequest( S, k ) @ #a) ∨
          (∃ #r. (LtkReveal( S ) @ #r) ∧ (#r < #i)))"
by sorry

lemma Client_auth_injective:
  all-traces
  "∀ S k #i.
         (SessKeyC( S, k ) @ #i) ⇒
         ((∃ #a.
            (AnswerRequest( S, k ) @ #a) ∧
            (∀ #j. (SessKeyC( S, k ) @ #j) ⇒ (#i = #j
          (∃ #r. (LtkReveal( S ) @ #r) ∧ (#r < #i)))"
by sorry

lemma Client_session_key_honest_setup:
  exists-trace
  "∃ S k #i.
         (SessKeyC( S, k ) @ #i) ∧ (¬(∃ #r. LtkReveal
simplify
solve( Client_1( S, k ) ▶₀ #i )
  case Client_1
  solve( !KU( h(~k) ) @ #vk )
    case Serv_1
    solve( !KU( aenc(~k, pk(~ltkS)) ) @ #vk.1 )
      case Client_1
      SOLVED // trace found
    qed
  qed
qed
```

Case: Client_1

Constraint System is Solved

Constraint system



last: none

formulas: ∀ #r. (LtkReveal($S) @ #r) ⇒ ⊥

subterms:

equations:
subst:
conj:

lemmas:

allowed cases: refined