Initial state
Game 1 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
let $mKt : mkey = \mathsf{mkgen}(rmKt)$ **in**
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $Nt : nonce$;
  new $ts : timest$;
  new $r1 : seed$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
  new $rAK : keyseed$;
  let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
  new $rmAK : mkeyseed$;
  let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
  new $r3 : seed$;
  let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
  let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
  new $r4 : seed$;
  let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
  let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
  let $q2 : bitstring = (hc, e4)$ **in**
  $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
|
  $!^{!_{13} \leq N}$
  $c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
  if $\mathsf{check}(m8, mKt, mac8)$ **then**
  let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
  if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
  let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
  event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
  $\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$
let $Rkey : key =$ **if** $(Khost = \mathsf{C})$ **then** Kc **else if** $(Khost = \mathsf{T})$ **then** Kt **else** $Kkey$ **in**
let $Rmkey : mkey =$ **if** $(Khost = \mathsf{C})$ **then** mKc **else if** $(Khost = \mathsf{T})$ **then** mKt **else** $Kmkey$
)

Applying expand if, let, find yields

Game 2 is
$start();$
new $rKc : keyseed;$
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed;$
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed;$
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed;$
let $mKt : mkey = \mathsf{mkgen}(rmKt)$ **in**
$\overline{c20}\langle\rangle;$
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host);$
new $Nc : nonce;$
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle;$
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs);$
if $\mathsf{check}(m2, mKc, mac2)$ **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $Nt : nonce;$
new $ts : timest;$
new $r1 : seed;$
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5);$
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce);$
find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed;$
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed;$
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed;$
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
new $r4 : seed;$
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
let $q2 : bitstring = (hc, e4)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
|
$!^{!_{13} \leq N}$

$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce);$
if $\mathsf{check}(m8, mKt, mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4) \rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$
if $(Khost = \mathsf{C})$ **then**
  let $Rkey : key = Kc$ **in**
  if $(Khost = \mathsf{C})$ **then**
    let $Rmkey : mkey = mKc$
  else
    if $(Khost = \mathsf{T})$ **then**
      let $Rmkey : mkey = mKt$
    else
      let $Rmkey : mkey = Kmkey$
else
  if $(Khost = \mathsf{T})$ **then**
    let $Rkey : key = Kt$ **in**
    if $(Khost = \mathsf{C})$ **then**
      let $Rmkey : mkey = mKc$
    else
      if $(Khost = \mathsf{T})$ **then**
        let $Rmkey : mkey = mKt$
      else
        let $Rmkey : mkey = Kmkey$
  else
    let $Rkey : key = Kkey$ **in**
    if $(Khost = \mathsf{C})$ **then**
      let $Rmkey : mkey = mKc$
    else
      if $(Khost = \mathsf{T})$ **then**
        let $Rmkey : mkey = mKt$
      else
        let $Rmkey : mkey = Kmkey$
)

Applying simplify yields

Game 3 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
let $mKt : mkey = \mathsf{mkgen}(rmKt)$ **in**
$\overline{c20}\langle\rangle$;

(
  !$^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc \rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $Nt : nonce$;
  new $ts : timest$;
  new $r1 : seed$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt \rangle$
|
  !$^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
  new $rAK : keyseed$;
  let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
  new $rmAK : mkeyseed$;
  let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
  new $r3 : seed$;
  let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
  let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
  new $r4 : seed$;
  let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
  let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
  let $q2 : bitstring = (hc, e4)$ **in**
  $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4 \rangle$
|
  !$^{!_{13} \leq N}$
  $c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
  if $\mathsf{check}(m8, mKt, mac8)$ **then**
  let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
  if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
  let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
  event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
  $\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4) \rangle$
|
  !$^{!_{14} \leq N2}$
  $c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
  if $(Khost = \mathsf{C})$ **then**
    let $Rkey : key = Kc$ **in**
    let $Rmkey : mkey = mKc$
  else
    if $(Khost = \mathsf{T})$ **then**
      let $Rkey : key = Kt$ **in**
      let $Rmkey : mkey = mKt$
    else
      let $Rkey : key = Kkey$ **in**
      let $Rmkey : mkey = Kmkey$

)

Applying move new all binders yields

Game 4 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
let $mKt : mkey = \mathsf{mkgen}(rmKt)$ **in**
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $r1 : seed$;
  new $ts : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
  new $rAK : keyseed$;
  let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
  new $rmAK : mkeyseed$;
  let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
  new $r3 : seed$;
  let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
  let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
  new $r4 : seed$;
  let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
  let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
  let $q2 : bitstring = (hc, e4)$ **in**
  $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
|
  $!^{!_{13} \leq N}$
  $c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
  if $\mathsf{check}(m8, mKt, mac8)$ **then**
  let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
  if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**

let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4) \rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey : mkey = mKc$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey : mkey = mKt$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey : mkey = Kmkey$
)

Applying remove assignments of useless yields

Game 5 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
let $mKt : mkey = \mathsf{mkgen}(rmKt)$ **in**
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc \rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
if $\mathsf{check}(m2, mKc, mac2)$ **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt \rangle$
|
$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat** **defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat** **defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**

new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
|
$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
if $\mathsf{check}(m8, mKt, mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
  let $Rkey : key = Kc$ **in**
  let $Rmkey : mkey = mKc$
else
  if $(Khost = \mathsf{T})$ **then**
    let $Rkey : key = Kt$ **in**
    let $Rmkey : mkey = mKt$
  else
    let $Rkey : key = Kkey$ **in**
    let $Rmkey : mkey = Kmkey$
)

Applying remove assignments of binder mKt yields

Game 6 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
if $\mathsf{check}(m2, mKc, mac2)$ **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**

new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
if $\mathsf{check}(m8, \mathsf{mkgen}(rmKt), mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
  let $Rkey : key = Kc$ **in**
  let $Rmkey : mkey = mKc$
else
  if $(Khost = \mathsf{T})$ **then**
    let $Rkey : key = Kt$ **in**
    let $Rmkey : mkey = \mathsf{mkgen}(rmKt)$
  else
    let $Rkey : key = Kkey$ **in**
    let $Rmkey : mkey = Kmkey$
)

Applying SA rename $Rmkey$ yields

Game 7 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**

new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $r1 : seed$;
  new $ts : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey_{28}[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{28}[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
      new $rmAK : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
      new $r3 : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{28}[j2])$ **in**
      new $r4 : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{28}[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
      new $rmAK : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
      new $r3 : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
      new $r4 : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{28}[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{30}[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
      new $rmAK : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**

new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{30}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{28}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey_{29}[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{28}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{28}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{30}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{30}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey_{30}[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{28}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{28}[j2])$ **in**
new $r4 : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{30}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{30}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{30}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK)$ **in**
new $rmAK : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK)$ **in**
new $r3 : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3)$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{30}[j2])$ **in**
new $r4 : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4)$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{30}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
if $\mathsf{check}(m8, \mathsf{mkgen}(rmKt), mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = mKc$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{mkgen}(rmKt)$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = Kmkey$

)

Applying remove assignments of binder *Rmkey* yields

Game 8 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $r1 : seed$;
  new $ts : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Kmkey[j1], Rmkey_{28}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
      new $r3_{33} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
      new $r4_{34} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{35} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
      new $rmAK_{36} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
      new $r3_{37} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
      new $r4_{38} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Khost[j1], Rkey[j1], Rmkey_{29}[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Rmkey_{29}[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**

new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Khost[j2], Rkey[j2], Rmkey_{29}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Rmkey_{29}[j2])$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
if $\mathsf{check}(m8, \mathsf{mkgen}(rmKt), mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{mkgen}(rmKt)$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$

)

Applying remove assignments of binder $Rmkey_{29}$ yields

Game 9 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $r1 : seed$;
  new $ts : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Kmkey[j1], Rmkey_{28}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
      new $r3_{33} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
      new $r4_{34} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{35} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
      new $rmAK_{36} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
      new $r3_{37} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKt))$ **in**
      new $r4_{38} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**

find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
if $\mathsf{check}(m8, \mathsf{mkgen}(rmKt), mac8)$ **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partT C}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**

let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying equivalence
$!^{N3}$ **new** $r : mkeyseed$; (
$!^{N}$ $(x : maxmac) \rightarrow \mathsf{mac}(x, \mathsf{mkgen}(r))$,
$!^{N2}$ $(m : maxmac, ma : macs) \rightarrow \mathsf{check}(m, \mathsf{mkgen}(r), ma)$)
$\approx_{N3 \times Pmac(\mathbf{time}, N, N2)}$
$!^{N3}$ **new** $r : mkeyseed$; (
$!^{N}$ $(x_{23} : maxmac) \rightarrow$ **let** $x : maxmac = x_{23}$ **in** $\mathsf{mac2}(x, \mathsf{mkgen2}(r))$,
$!^{N2}$ $(m : maxmac, ma : macs) \rightarrow$ **find** $j \leq N$ **suchthat defined**$(x[j]) \wedge ((m = x[j]) \wedge \mathsf{check2}(x[j], \mathsf{mkgen2}(r), ma))$ **then** true
else false)
with $rmKt$ [Difference of probability $Pmac(\mathbf{time} + \mathbf{time}(context\ for\ game\ 9), 2. \times N, N)$] yields

Game 10 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc \rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
if $\mathsf{check}(m2, mKc, mac2)$ **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt \rangle$
|
$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Kmkey[j1], Rmkey_{28}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**

let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{67}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{68}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{70}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{69}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{71}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kmkey[j2], Rmkey_{28}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(rmKt, Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{72}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(mKc, Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce);$
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}]) \wedge ((m8 = x_{67}[@i_{78}]) \wedge \mathsf{check2}(x_{67}[@i_{78}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}]) \wedge ((m8 = x_{68}[@i_{77}]) \wedge \mathsf{check2}(x_{68}[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}]) \wedge ((m8 = x_{69}[@i_{76}]) \wedge \mathsf{check2}(x_{69}[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}]) \wedge ((m8 = x_{70}[@i_{75}]) \wedge \mathsf{check2}(x_{70}[@i_{75}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}]) \wedge ((m8 = x_{71}[@i_{74}]) \wedge \mathsf{check2}(x_{71}[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}]) \wedge ((m8 = x_{72}[@i_{73}]) \wedge \mathsf{check2}(x_{72}[@i_{73}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if true **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
else
if false **then**
let $injbot(concat2(AK_{16} : key, mAK_{15} : mkey, h4 : host)) = \mathsf{dec}(m8, Kt)$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|
  !$^{!_{14} \leq N2}$
  $c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
  if $(Khost = \mathsf{C})$ **then**
    let $Rkey : key = Kc$ **in**
    let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
  else
    if $(Khost = \mathsf{T})$ **then**
      let $Rkey : key = Kt$ **in**
      let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
    else
      let $Rkey : key = Kkey$ **in**
      let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying simplify yields

Game 11 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  !$^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $r1 : seed$;
  new $ts : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  !$^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
      new $r3_{33} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**

let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{67}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{68}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{70}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{69}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{71}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{72}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$

$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce);$

find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}]) \wedge ((m8 = x_{67}[@i_{78}]) \wedge \mathsf{check2}(x_{67}[@i_{78}], \mathsf{mkge}$

let $AK_{16} : key = AK_{17}[@i_{78}]$ **in**

let $mAK_{15} : mkey = mAK_{18}[@i_{78}]$ **in**

let $h4 : host = hc[@i_{78}]$ **in**

if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**

let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**

event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;

$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}]) \wedge ((m8 = x_{68}[@i_{77}]) \wedge \mathsf{check2}(x_{68}[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**

$\overline{0}$

$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}]) \wedge ((m8 = x_{69}[@i_{76}]) \wedge \mathsf{check2}(x_{69}[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**

$\overline{0}$

$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}]) \wedge ((m8 = x_{70}[@i_{75}]) \wedge \mathsf{check2}(x_{70}[@i_{75}], \mathsf{mkgen2}$

let $AK_{16} : key = AK_{17}[@i_{75}]$ **in**

let $mAK_{15} : mkey = mAK_{18}[@i_{75}]$ **in**

let $h4 : host = hc[@i_{75}]$ **in**

if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**

let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**

event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;

$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}]) \wedge ((m8 = x_{71}[@i_{74}]) \wedge \mathsf{check2}(x_{71}[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**

$\overline{0}$

$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}]) \wedge ((m8 = x_{72}[@i_{73}]) \wedge \mathsf{check2}(x_{72}[@i_{73}], \mathsf{mkgen2}$

let $AK_{16} : key = AK_{17}[@i_{73}]$ **in**

let $mAK_{15} : mkey = mAK_{18}[@i_{73}]$ **in**

let $h4 : host = hc[@i_{73}]$ **in**

if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**

let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**

event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;

$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$

|

$!^{!_{14} \leq N2}$

$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$

if $(Khost = \mathsf{C})$ **then**

let $Rkey : key = Kc$ **in**

let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$

else

if $(Khost = \mathsf{T})$ **then**

let $Rkey : key = Kt$ **in**

let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$

else

let $Rkey : key = Kkey$ **in**

let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$

)

Applying move new all binders yields

Game 12 is

$start();$

new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, mKc, mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $ts : timest$;
  new $r1 : seed$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
      new $r3_{33} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
      new $r4_{34} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{35} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
      new $rmAK_{36} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
      new $r3_{37} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
      let $x_{67} : maxmac = e3$ **in**
      let $mac3 : macs = \mathsf{mac2}(x_{67}, \mathsf{mkgen2}(rmKt))$ **in**
      new $r4_{38} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{39} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{68}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{70}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{69}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{71}, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{72}, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}]) \wedge ((m8 = x_{67}[@i_{78}]) \wedge \mathsf{check2}(x_{67}[@i_{78}], \mathsf{mkge}$
let $AK_{16} : key = AK_{17}[@i_{78}]$ **in**
let $mAK_{15} : mkey = mAK_{18}[@i_{78}]$ **in**
let $h4 : host = hc[@i_{78}]$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}]) \wedge ((m8 = x_{68}[@i_{77}]) \wedge \mathsf{check2}(x_{68}[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}]) \wedge ((m8 = x_{69}[@i_{76}]) \wedge \mathsf{check2}(x_{69}[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}]) \wedge ((m8 = x_{70}[@i_{75}]) \wedge \mathsf{check2}(x_{70}[@i_{75}], \mathsf{mkgen2}$
let $AK_{16} : key = AK_{17}[@i_{75}]$ **in**
let $mAK_{15} : mkey = mAK_{18}[@i_{75}]$ **in**
let $h4 : host = hc[@i_{75}]$ **in**

if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}]) \wedge ((m8 = x_{71}[@i_{74}]) \wedge \mathsf{check2}(x_{71}[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}]) \wedge ((m8 = x_{72}[@i_{73}]) \wedge \mathsf{check2}(x_{72}[@i_{73}], \mathsf{mkgen2}$
let $AK_{16} : key = AK_{17}[@i_{73}]$ **in**
let $mAK_{15} : mkey = mAK_{18}[@i_{73}]$ **in**
let $h4 : host = hc[@i_{73}]$ **in**
if $\mathsf{check}(m9, mAK_{15}, mac9)$ **then**
let $injbot(pad(= h4, t : timest)) = \mathsf{dec}(m9, AK_{16})$ **in**
event $\mathsf{partTC}(h4, AK_{16}, mAK_{15}, m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(h4)\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of useless yields

Game 13 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
let $mKc : mkey = \mathsf{mkgen}(rmKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
if $\mathsf{check}(m2, mKc, mac2)$ **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**

event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
    new $rAK_{31} : keyseed$;
    let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
    new $rmAK_{32} : mkeyseed$;
    let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
    new $r3_{33} : seed$;
    let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
    let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
    new $r4_{34} : seed$;
    let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
    let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
    $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
  $\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
    new $rAK_{35} : keyseed$;
    let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
    new $rmAK_{36} : mkeyseed$;
    let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
    new $r3_{37} : seed$;
    let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
    let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
    let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
    new $r4_{38} : seed$;
    let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
    let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
    $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
  $\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
    new $rAK_{39} : keyseed$;
    let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
    new $rmAK_{40} : mkeyseed$;
    let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
    new $r3_{41} : seed$;
    let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
    let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
    new $r4_{42} : seed$;
    let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
    let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
    $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
    new $rAK_{43} : keyseed$;
    let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
    new $rmAK_{44} : mkeyseed$;
    let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
    new $r3_{45} : seed$;
    let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
    let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
    new $r4_{46} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, mKc)$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, mKc)$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

!$^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(e3[@i_{78}], x_{67}[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(e4[@i_{77}], x_{68}[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(e4[@i_{76}], x_{69}[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(e3[@i_{75}], x_{70}[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(e4[@i_{74}], x_{71}[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(e3[@i_{73}], x_{72}[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

!$^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of binder mKc yields

Game 14 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  if $\mathsf{check}(m2, \mathsf{mkgen}(rmKc), mac2)$ **then**
  let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
  new $ts : timest$;
  new $r1 : seed$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
  event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
  new $Nt : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
      new $r3_{33} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
      let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
      new $r4_{34} : seed$;
      let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
      let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
      $\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
    $\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{35} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
      new $rmAK_{36} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
      new $r3_{37} : seed$;
      let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
      let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
      let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
      new $r4_{38} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, \mathsf{mkgen}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, \mathsf{mkgen}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(e3[@i_{78}], x_{67}[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(e4[@i_{77}], x_{68}[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(e4[@i_{76}], x_{69}[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(e3[@i_{75}], x_{70}[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$

if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(e4[@i_{74}], x_{71}[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(e3[@i_{73}], x_{72}[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying equivalence
$!^{N3}$ **new** $r : mkeyseed$; (
$!^{N}$ $(x : maxmac) \rightarrow \mathsf{mac}(x, \mathsf{mkgen}(r))$,
$!^{N2}$ $(m : maxmac, ma : macs) \rightarrow \mathsf{check}(m, \mathsf{mkgen}(r), ma)$)
$\approx_{N3 \times Pmac(\mathbf{time}, N, N2)}$
$!^{N3}$ **new** $r : mkeyseed$; (
$!^{N}$ $(x_{23} : maxmac) \rightarrow$ **let** $x : maxmac = x_{23}$ **in** $\mathsf{mac2}(x, \mathsf{mkgen2}(r))$,
$!^{N2}$ $(m : maxmac, ma : macs) \rightarrow$ **find** $j \leq N$ **suchthat defined**$(x[j]) \wedge ((m = x[j]) \wedge \mathsf{check2}(x[j], \mathsf{mkgen2}(r), ma))$ **then** true
else false)
with $rmKc$ [Difference of probability $Pmac(\mathbf{time} + \mathbf{time}(context\ for\ game\ 14), 2. \times N, N)$] yields

Game 15 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}]) \wedge ((m2 = x_{173}[@i_{185}]) \wedge \mathsf{check2}(x_{173}[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **then**

if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}]) \wedge ((m2 = x_{174}[@i_{184}]) \wedge \mathsf{check2}(x_{174}[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}]) \wedge ((m2 = x_{175}[@i_{183}]) \wedge \mathsf{check2}(x_{175}[@i_{183}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}]) \wedge ((m2 = x_{176}[@i_{182}]) \wedge \mathsf{check2}(x_{176}[@i_{182}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}]) \wedge ((m2 = x_{177}[@i_{181}]) \wedge \mathsf{check2}(x_{177}[@i_{181}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}]) \wedge ((m2 = x_{178}[@i_{180}]) \wedge \mathsf{check2}(x_{178}[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if true **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;

new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
else
if false **then**
let $injbot(concat1(AK_{20} : key, mAK_{19} : mkey, = Nc, = h)) = \mathsf{dec}(m2, Kc)$ **in**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
|
$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $x_{173} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{173}, \mathsf{mkgen2}(rmKc))$ **in**

new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $x_{174} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{174}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**

let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $x_{175} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{175}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $x_{176} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{176}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $x_{178} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{178}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $x_{177} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{177}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(e3[@i_{78}], x_{67}[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$

$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(e4[@i_{77}], x_{68}[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(e4[@i_{76}], x_{69}[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(e3[@i_{75}], x_{70}[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$

$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(e4[@i_{74}], x_{71}[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(e3[@i_{73}], x_{72}[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying simplify yields

Game 16 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rmKc : mkeyseed$;
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}]) \wedge ((m2 = x_{173}[@i_{185}]) \wedge \mathsf{check2}(x_{173}[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}]) \wedge ((m2 = x_{174}[@i_{184}]) \wedge \mathsf{check2}(x_{174}[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = x_{175}[@i_{183}]) \wedge \mathsf{check2}(x$
let $AK_{20} : key = AK_{17}[@i_{183}]$ **in**
let $mAK_{19} : mkey = mAK_{18}[@i_{183}]$ **in**
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$

$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = x_{176}[@i_{182}]) \wedge \mathsf{check2}(x$
let $AK_{20} : key = AK_{17}[@i_{182}]$ **in**
let $mAK_{19} : mkey = mAK_{18}[@i_{182}]$ **in**
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = x_{177}[@i_{181}]) \wedge \mathsf{check2}(x$
let $AK_{20} : key = AK_{17}[@i_{181}]$ **in**
let $mAK_{19} : mkey = mAK_{18}[@i_{181}]$ **in**
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $ts : timest$;
new $r1 : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}]) \wedge ((m2 = x_{178}[@i_{180}]) \wedge \mathsf{check2}(x_{178}[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $x_{173} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{173}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $x_{174} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{174}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $x_{175} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{175}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $x_{176} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{176}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $x_{178} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{178}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $x_{177} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{177}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$

$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**

$\overline{0}$
$\oplus$ @$i_{76} \leq N$ **suchthat defined**(x_{69}[@i_{76}], *e4*[@i_{76}]) $\wedge$ ((*m8* = *e4*[@i_{76}]) $\wedge$ check2(*e4*[@i_{76}], mkgen2(*rmKt*), *mac8*)) **then**
$\overline{0}$
$\oplus$ @$i_{75} \leq N$ **suchthat defined**(x_{70}[@i_{75}], *e3*[@i_{75}], mAK_{18}[@i_{75}], *hc*[@i_{75}], AK_{17}[@i_{75}]) $\wedge$ ((*m8* = *e3*[@i_{75}]) $\wedge$ check2(*e3*[@i_{75}]
if check(*m9*, mAK_{18}[@i_{75}], *mac9*) **then**
let *injbot*(*pad*(= *hc*[@i_{75}], *t* : *timest*)) = dec(*m9*, AK_{17}[@i_{75}]) **in**
event partTC(*hc*[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], *m8*, *m9*);
$\overline{c8[!_{13}]}\langle$acceptT(*hc*[@$i_{75}$])$\rangle$
$\oplus$ @$i_{74} \leq N$ **suchthat defined**(x_{71}[@i_{74}], *e4*[@i_{74}]) $\wedge$ ((*m8* = *e4*[@i_{74}]) $\wedge$ check2(*e4*[@i_{74}], mkgen2(*rmKt*), *mac8*)) **then**
$\overline{0}$
$\oplus$ @$i_{73} \leq N$ **suchthat defined**(x_{72}[@i_{73}], *e3*[@i_{73}], mAK_{18}[@i_{73}], *hc*[@i_{73}], AK_{17}[@i_{73}]) $\wedge$ ((*m8* = *e3*[@i_{73}]) $\wedge$ check2(*e3*[@i_{73}]
if check(*m9*, mAK_{18}[@i_{73}], *mac9*) **then**
let *injbot*(*pad*(= *hc*[@i_{73}], *t* : *timest*)) = dec(*m9*, AK_{17}[@i_{73}]) **in**
event partTC(*hc*[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], *m8*, *m9*);
$\overline{c8[!_{13}]}\langle$acceptT(*hc*[@$i_{73}$])$\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if (*Khost* = T) **then**
let *Rkey* : *key* = *Kc* **in**
let $Rmkey_{30}$: *mkey* = cst_mkey
else
if (*Khost* = T) **then**
let *Rkey* : *key* = *Kt* **in**
let $Rmkey_{29}$: *mkey* = cst_mkey
else
let *Rkey* : *key* = *Kkey* **in**
let $Rmkey_{28}$: *mkey* = cst_mkey
)

Applying move new all binders yields

Game 17 is
start();
new *rKc* : *keyseed*;
let *Kc* : *key* = kgen(*rKc*) **in**
new *rKt* : *keyseed*;
let *Kt* : *key* = kgen(*rKt*) **in**
new *rmKt* : *mkeyseed*;
new *rmKc* : *mkeyseed*;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new *Nc* : *nonce*;
$\overline{c2[!_{11}]}\langle$T, *h*, *Nc*$\rangle$;
$c3[!_{11}](=$ T, *m* : *maxmac*, *mac1* : *macs*, *m2* : *maxmac*, *mac2* : *macs*);
find @$i_{185} \leq N$ **suchthat defined**(x_{173}[@i_{185}]) $\wedge$ ((*m2* = x_{173}[@i_{185}]) $\wedge$ check2(x_{173}[@i_{185}], mkgen2(*rmKc*), *mac2*)) **then**
$\overline{0}$
$\oplus$ @$i_{184} \leq N$ **suchthat defined**(x_{174}[@i_{184}]) $\wedge$ ((*m2* = x_{174}[@i_{184}]) $\wedge$ check2(x_{174}[@i_{184}], mkgen2(*rmKc*), *mac2*)) **then**
$\overline{0}$
$\oplus$ @$i_{183} \leq N$ **suchthat defined**(x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], *n*[@i_{183}], *ht*[@i_{183}]) $\wedge$ ((*m2* = x_{175}[@i_{183}]) $\wedge$ check2(*x*
let AK_{20} : *key* = AK_{17}[@i_{183}] **in**

let $mAK_{19} : mkey = mAK_{18}[@i_{183}]$ **in**
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = x_{176}[@i_{182}]) \wedge \mathsf{check2}($x
let $AK_{20} : key = AK_{17}[@i_{182}]$ **in**
let $mAK_{19} : mkey = mAK_{18}[@i_{182}]$ **in**
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = x_{177}[@i_{181}]) \wedge \mathsf{check2}($x
let $AK_{20} : key = AK_{17}[@i_{181}]$ **in**
let $mAK_{19} : mkey = mAK_{18}[@i_{181}]$ **in**
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $r1 : seed$;
new $ts : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts), AK_{20}, r1)$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{19})$ **in**
event $\mathsf{partCT}(h, AK_{20}, mAK_{19}, m, e5)$;
new $Nt : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}]) \wedge ((m2 = x_{178}[@i_{180}]) \wedge \mathsf{check2}(x_{178}[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $x_{173} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{173}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $x_{174} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{174}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $x_{175} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{175}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $x_{176} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{176}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $x_{178} : maxmac = e3$ **in**
let $mac3 : macs = \mathsf{mac2}(x_{178}, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**
let $x_{177} : maxmac = e4$ **in**
let $mac4 : macs = \mathsf{mac2}(x_{177}, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|
  $!^{!_{13} \leq N}$
  $c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
  find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
    if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
    let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
    event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
    $\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}]) \rangle$
  $\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
    if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
    let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
    event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
    $\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}]) \rangle$
  $\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
    if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
    let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
    event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
    $\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}]) \rangle$
|
  $!^{!_{14} \leq N2}$
  $c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
  if $(Khost = \mathsf{C})$ **then**
    let $Rkey : key = Kc$ **in**
    let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
  else
    if $(Khost = \mathsf{T})$ **then**
      let $Rkey : key = Kt$ **in**
      let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
    else
      let $Rkey : key = Kkey$ **in**
      let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of useless yields

Game 18 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;

new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(e3[@i_{185}], x_{173}[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
  $\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(e3[@i_{184}], x_{174}[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
  $\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(e4[@i_{183}], x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
  if $(Nc = n[@i_{183}])$ **then**
  if $(h = ht[@i_{183}])$ **then**
  new $r1_{190} : seed$;
  new $ts_{191} : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
  event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
  new $Nt_{192} : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(e4[@i_{182}], x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
  if $(Nc = n[@i_{182}])$ **then**
  if $(h = ht[@i_{182}])$ **then**
  new $r1_{193} : seed$;
  new $ts_{194} : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
  event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
  new $Nt_{195} : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(e4[@i_{181}], x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
  if $(Nc = n[@i_{181}])$ **then**
  if $(h = ht[@i_{181}])$ **then**
  new $r1_{196} : seed$;
  new $ts_{197} : timest$;
  let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
  let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
  event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
  new $Nt_{198} : nonce$;
  $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(e3[@i_{180}], x_{178}[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
  $\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
  find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
    new $rAK_{31} : keyseed$;
    let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
    new $rmAK_{32} : mkeyseed$;
    let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
    new $r3_{33} : seed$;
    let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{33})$ **in**
    let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
    new $r4_{34} : seed$;
    let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{34})$ **in**
    let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey[j2], r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey[j1], r4_{66})$ **in**

let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce);$
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9);$
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9);$
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9);$
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$
if $(Khost = \mathsf{C})$ **then**
let $Rkey : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying SA rename *Rkey* yields

Game 19 is
$start();$
new $rKc : keyseed;$
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rKt : keyseed;$
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed;$
new $rmKc : mkeyseed;$
$\overline{c20}\langle\rangle;$

(
!$^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc \rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(e3[@i_{185}], x_{173}[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(e3[@i_{184}], x_{174}[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(e4[@i_{183}], x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $r1_{190} : seed$;
new $ts_{191} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192} \rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(e4[@i_{182}], x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $r1_{193} : seed$;
new $ts_{194} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195} \rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(e4[@i_{181}], x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $r1_{196} : seed$;
new $ts_{197} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198} \rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(e3[@i_{180}], x_{178}[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
|
!$^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Rkey_{288}[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey_{288}[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{288}[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**

new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{288}[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey_{289}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{289}[j2], r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{288}[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey_{290}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{290}[j2], r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{288}[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1], Rkey_{289}[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey_{288}[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{288}[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{289}[j1], r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey_{289}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{289}[j2], r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{289}[j1], r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey_{290}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{290}[j2], r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{289}[j1], r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1], Rkey_{290}[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Rkey_{288}[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{288}[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{290}[j1], r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2], Rkey_{289}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{289}[j2], r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{290}[j1], r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2], Rkey_{290}[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Rkey_{290}[j2], r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Rkey_{290}[j1], r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = Kc$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = Kt$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey_{288} : key = Kkey$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$

)

Applying remove assignments of binder $Rkey$ yields

Game 20 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{kgen}(rKc)$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**

new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  find $@i_{185} \leq N$ **suchthat defined**$(e3[@i_{185}], x_{173}[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
    $\overline{0}$
  $\oplus$ $@i_{184} \leq N$ **suchthat defined**$(e3[@i_{184}], x_{174}[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{183} \leq N$ **suchthat defined**$(e4[@i_{183}], x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
    if $(Nc = n[@i_{183}])$ **then**
    if $(h = ht[@i_{183}])$ **then**
    new $r1_{190} : seed$;
    new $ts_{191} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
    new $Nt_{192} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
  $\oplus$ $@i_{182} \leq N$ **suchthat defined**$(e4[@i_{182}], x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
    if $(Nc = n[@i_{182}])$ **then**
    if $(h = ht[@i_{182}])$ **then**
    new $r1_{193} : seed$;
    new $ts_{194} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
    new $Nt_{195} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
  $\oplus$ $@i_{181} \leq N$ **suchthat defined**$(e4[@i_{181}], x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
    if $(Nc = n[@i_{181}])$ **then**
    if $(h = ht[@i_{181}])$ **then**
    new $r1_{196} : seed$;
    new $ts_{197} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
    new $Nt_{198} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
  $\oplus$ $@i_{180} \leq N$ **suchthat defined**$(e3[@i_{180}], x_{178}[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
    $\overline{0}$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Kkey[j1], Rkey_{288}[j1], Rmkey_{28}[j1], Khost[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;
      let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
      new $rmAK_{32} : mkeyseed$;
      let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**

new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kc, r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j1], Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**

let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kc, r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Kc, Rkey_{290}[j1], Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kc, r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kc, r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**

new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kc, r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kc, r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey_{288} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of binder Kc yields

Game 21 is
$start()$;
new $rKc : keyseed$;

let $Kc : key = \mathsf{cst\_key}$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
  $!^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  find $@i_{185} \leq N$ **suchthat defined**$(e3[@i_{185}], x_{173}[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
    $\overline{0}$
  $\oplus$ $@i_{184} \leq N$ **suchthat defined**$(e3[@i_{184}], x_{174}[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{183} \leq N$ **suchthat defined**$(e4[@i_{183}], x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
    if $(Nc = n[@i_{183}])$ **then**
    if $(h = ht[@i_{183}])$ **then**
    new $r1_{190} : seed$;
    new $ts_{191} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
    new $Nt_{192} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
  $\oplus$ $@i_{182} \leq N$ **suchthat defined**$(e4[@i_{182}], x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
    if $(Nc = n[@i_{182}])$ **then**
    if $(h = ht[@i_{182}])$ **then**
    new $r1_{193} : seed$;
    new $ts_{194} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
    new $Nt_{195} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
  $\oplus$ $@i_{181} \leq N$ **suchthat defined**$(e4[@i_{181}], x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
    if $(Nc = n[@i_{181}])$ **then**
    if $(h = ht[@i_{181}])$ **then**
    new $r1_{196} : seed$;
    new $ts_{197} : timest$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
    new $Nt_{198} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
  $\oplus$ $@i_{180} \leq N$ **suchthat defined**$(e3[@i_{180}], x_{178}[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
    $\overline{0}$
|
  $!^{!_{12} \leq N}$
  $c14[!_{12}](hc : host, ht : host, n : nonce)$;
  find $j1 \leq N2$ **suchthat defined**$(Kkey[j1], Rkey_{288}[j1], Rmkey_{28}[j1], Khost[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
    find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
      new $rAK_{31} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j1], Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;

let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j1], Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey_{288} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying equivalence
$!^{N2}$ **new** $r : keyseed$; $!^{N}$ **new** $r2 : seed$; $(x : maxenc) \rightarrow \mathsf{enc}(x, \mathsf{kgen}(r), r2)$

$\approx_{N2 \times Penc(\mathbf{time},N)}$
$!^{N2}$ **new** $r : keyseed$; $!^{N}$ **new** $r2 : seed$; $(x : maxenc) \rightarrow \mathsf{enc2}(\mathsf{Z}(x), \mathsf{kgen2}(r), r2)$
with $r4_{66}$ [Difference of probability $Penc(\mathbf{time} + \mathbf{time}(\textit{context for game } 21), 2. \times N)$] yields

Game 22 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{cst\_key}$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(e3[@i_{185}], x_{173}[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(e3[@i_{184}], x_{174}[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(e4[@i_{183}], x_{175}[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}], n[@i_{183}], ht[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $r1_{190} : seed$;
new $ts_{191} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(e4[@i_{182}], x_{176}[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}], n[@i_{182}], ht[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $r1_{193} : seed$;
new $ts_{194} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(e4[@i_{181}], x_{177}[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}], n[@i_{181}], ht[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $r1_{196} : seed$;
new $ts_{197} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(e3[@i_{180}], x_{178}[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**

$\overline{0}$

|

$!^{!_{12} \leq N}$

$c14[!_{12}](hc : host, ht : host, n : nonce);$

find $j1 \leq N2$ **suchthat defined**$(Kkey[j1], Rkey_{288}[j1], Rmkey_{28}[j1], Khost[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**

find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{31} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**

new $rmAK_{32} : mkeyseed$;

let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**

new $r3_{33} : seed$;

let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**

let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**

new $r4_{34} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**

let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{35} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**

new $rmAK_{36} : mkeyseed$;

let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**

new $r3_{37} : seed$;

let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**

let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**

new $r4_{38} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**

let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{39} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**

new $rmAK_{40} : mkeyseed$;

let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**

new $r3_{41} : seed$;

let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKc), r3_{41})$ **in**

let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**

new $r4_{42} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**

let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j1 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j1], Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**

find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{43} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**

new $rmAK_{44} : mkeyseed$;

let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**

new $r3_{45} : seed$;

let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**

let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**

new $r4_{46} : seed$;

let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**

let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j1], Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Kkey[j2], Rkey_{288}[j2], Rmkey_{28}[j2], Khost[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Kt, Rkey_{289}[j2], Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**

new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(rKc, Kc, Rkey_{290}[j2], Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$

else
let $Rkey_{288} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying simplify yields

Game 23 is
$start()$;
new $rKc : keyseed$;
let $Kc : key = \mathsf{cst\_key}$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
$\overline{c20}\langle\rangle$;
(
! $^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $r1_{190} : seed$;
new $ts_{191} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $r1_{193} : seed$;
new $ts_{194} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $r1_{196} : seed$;
new $ts_{197} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**

event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;

let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**

new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$

else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey_{288} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying move new all binders yields

Game 24 is
$start()$;
let $Kc : key = \mathsf{cst\_key}$ **in**
new $rKt : keyseed$;
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKc : mkeyseed$;
new $rmKt : mkeyseed$;
new $rKc : keyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $ts_{191} : timest$;
new $r1_{190} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $ts_{194} : timest$;
new $r1_{193} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**

new $ts_{197} : timest$;
new $r1_{196} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;

let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|

$!^{!_{14} \leq N2}$

$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$
if $(Khost = \mathsf{C})$ **then**
let $Rkey_{290} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rkey_{289} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rkey_{288} : key = \mathsf{cst\_key}$ **in**
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of useless yields

Game 25 is
$start();$
new $rKt : keyseed;$
let $Kt : key = \mathsf{kgen}(rKt)$ **in**
new $rmKc : mkeyseed;$
new $rmKt : mkeyseed;$
new $rKc : keyseed;$
$\overline{c20}\langle\rangle;$
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host);$
new $Nc : nonce;$
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle;$
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs);$
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $ts_{191} : timest;$
new $r1_{190} : seed;$
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5);$
new $Nt_{192} : nonce;$
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $ts_{194} : timest;$
new $r1_{193} : seed;$
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5);$
new $Nt_{195} : nonce;$
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$

$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $ts_{197} : timest$;
new $r1_{196} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ *j1* $\leq$ *N2* **suchthat defined**($Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kt, r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j1* $\leq$ *N2* **suchthat defined**($Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kt, r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;

$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey);$
if $(Khost = \mathsf{C})$ **then**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying remove assignments of binder Kt yields

Game 26 is
$start();$
new $rKt : keyseed;$
new $rmKc : mkeyseed;$
new $rmKt : mkeyseed;$
new $rKc : keyseed;$
$\overline{c20}\langle\rangle;$
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host);$
new $Nc : nonce;$
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle;$
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs);$
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $ts_{191} : timest;$
new $r1_{190} : seed;$
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5);$
new $Nt_{192} : nonce;$
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $ts_{194} : timest;$
new $r1_{193} : seed;$
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5);$
new $Nt_{195} : nonce;$
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$

if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $ts_{197} : timest$;
new $r1_{196} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKt), r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**

find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKt), r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKt), r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKt), r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), \mathsf{kgen}(rKt), r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), \mathsf{kgen}(rKt), r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$

|
  !$^{!_{14} \leq N2}$
  $c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
  if $(Khost = \mathsf{C})$ **then**
    let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
  else
    if $(Khost = \mathsf{T})$ **then**
      let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
    else
      let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying equivalence
!^{N2} **new** $r : keyseed$; !^{N} **new** $r2 : seed$; $(x : maxenc) \rightarrow \mathsf{enc}(x, \mathsf{kgen}(r), r2)$
$\approx_{N2 \times Penc(\mathbf{time}, N)}$
!^{N2} **new** $r : keyseed$; !^{N} **new** $r2 : seed$; $(x : maxenc) \rightarrow \mathsf{enc2}(\mathsf{Z}(x), \mathsf{kgen2}(r), r2)$
with $r3_{61}$ [Difference of probability $Penc(\mathbf{time} + \mathbf{time}(context\ for\ game\ 26), 2. \times N)$] yields

Game 27 is
$start()$;
new $rKt : keyseed$;
new $rmKc : mkeyseed$;
new $rmKt : mkeyseed$;
new $rKc : keyseed$;
$\overline{c20}\langle\rangle$;
(
  !$^{!_{11} \leq N}$
  $c1[!_{11}](h : host)$;
  new $Nc : nonce$;
  $\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc \rangle$;
  $c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
  find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
    $\overline{0}$
  $\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
    $\overline{0}$
  $\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
    if $(Nc = n[@i_{183}])$ **then**
    if $(h = ht[@i_{183}])$ **then**
    new $ts_{191} : timest$;
    new $r1_{190} : seed$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
    new $Nt_{192} : nonce$;
    $\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192} \rangle$
  $\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
    if $(Nc = n[@i_{182}])$ **then**
    if $(h = ht[@i_{182}])$ **then**
    new $ts_{194} : timest$;
    new $r1_{193} : seed$;
    let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
    let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
    event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;

new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $ts_{197} : timest$;
new $r1_{196} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKt), r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**

let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKt), r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKt), r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKt), r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht)), \mathsf{kgen2}(rKt), r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;

let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Z}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc)), \mathsf{kgen2}(rKt), r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$

$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$

$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$

$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**

let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**
event $\mathsf{partTC}(hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{73}])\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost = \mathsf{C})$ **then**
let $Rmkey_{30} : mkey = \mathsf{cst\_mkey}$
else
if $(Khost = \mathsf{T})$ **then**
let $Rmkey_{29} : mkey = \mathsf{cst\_mkey}$
else
let $Rmkey_{28} : mkey = \mathsf{cst\_mkey}$
)

Applying simplify yields

Game 28 is
$start()$;
new $rKt : keyseed$;
new $rmKc : mkeyseed$;
new $rmKt : mkeyseed$;
new $rKc : keyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle \mathsf{C}, h, Nc\rangle$;
$c3[!_{11}](= \mathsf{C}, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat** **defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge \mathsf{check2}(e3[@i_{185}], \mathsf{mkgen2}(rmKc), mac2))$ **the**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat** **defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge \mathsf{check2}(e3[@i_{184}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat** **defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $ts_{191} : timest$;
new $r1_{190} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{191}), AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{183}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat** **defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $ts_{194} : timest$;
new $r1_{193} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;

$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge$
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $ts_{197} : timest$;
new $r1_{196} : seed$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**

$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j1* $\leq$ *N2* **suchthat defined**($Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ *j1* $\leq$ *N2* **suchthat defined**($Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find *j2* $\leq$ *N2* **suchthat defined**($Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**

let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$

|

$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge \mathsf{check2}(e3[@i$
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**
event $\mathsf{partTC}(hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{78}])\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**$(x_{68}[@i_{77}], e4[@i_{77}]) \wedge ((m8 = e4[@i_{77}]) \wedge \mathsf{check2}(e4[@i_{77}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**$(x_{69}[@i_{76}], e4[@i_{76}]) \wedge ((m8 = e4[@i_{76}]) \wedge \mathsf{check2}(e4[@i_{76}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**$(x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]) \wedge ((m8 = e3[@i_{75}]) \wedge \mathsf{check2}(e3[@i_{75}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{75}], mac9)$ **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{75}])$ **in**
event $\mathsf{partTC}(hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9)$;
$\overline{c8[!_{13}]}\langle \mathsf{acceptT}(hc[@i_{75}])\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**$(x_{71}[@i_{74}], e4[@i_{74}]) \wedge ((m8 = e4[@i_{74}]) \wedge \mathsf{check2}(e4[@i_{74}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**$(x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]) \wedge ((m8 = e3[@i_{73}]) \wedge \mathsf{check2}(e3[@i_{73}]$
if $\mathsf{check}(m9, mAK_{18}[@i_{73}], mac9)$ **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{73}])$ **in**

event partTC($hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9$);
$\overline{c8[!_{13}]}\langle$acceptT($hc[@i_{73}]$)$\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if $(Khost =$ C$)$ **then**
let $Rmkey_{30} : mkey =$ cst_mkey
else
if $(Khost =$ T$)$ **then**
let $Rmkey_{29} : mkey =$ cst_mkey
else
let $Rmkey_{28} : mkey =$ cst_mkey
)

Applying move new all binders yields

Game 29 is
$start()$;
new $rKc : keyseed$;
new $rmKt : mkeyseed$;
new $rmKc : mkeyseed$;
new $rKt : keyseed$;
$\overline{c20}\langle\rangle$;
(
$!^{!_{11} \leq N}$
$c1[!_{11}](h : host)$;
new $Nc : nonce$;
$\overline{c2[!_{11}]}\langle$C$, h, Nc\rangle$;
$c3[!_{11}](=$ C$, m : maxmac, mac1 : macs, m2 : maxmac, mac2 : macs)$;
find $@i_{185} \leq N$ **suchthat defined**$(x_{173}[@i_{185}], e3[@i_{185}]) \wedge ((m2 = e3[@i_{185}]) \wedge$ check2$(e3[@i_{185}],$ mkgen2$(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{184} \leq N$ **suchthat defined**$(x_{174}[@i_{184}], e3[@i_{184}]) \wedge ((m2 = e3[@i_{184}]) \wedge$ check2$(e3[@i_{184}],$ mkgen2$(rmKc), mac2))$ **then**
$\overline{0}$
$\oplus$ $@i_{183} \leq N$ **suchthat defined**$(x_{175}[@i_{183}], e4[@i_{183}], n[@i_{183}], ht[@i_{183}], AK_{17}[@i_{183}], mAK_{18}[@i_{183}]) \wedge ((m2 = e4[@i_{183}]) \wedge$ check2$(e4[@i_{183}],$ mkgen2$(rmKc), mac2))$ **then**
if $(Nc = n[@i_{183}])$ **then**
if $(h = ht[@i_{183}])$ **then**
new $r1_{190} : seed$;
new $ts_{191} : timest$;
let $e5 : maxmac =$ enc(pad(C, ts_{191}), $AK_{17}[@i_{183}], r1_{190})$ **in**
let $mac5 : macs =$ mac$(e5, mAK_{18}[@i_{183}])$ **in**
event partCT$(h, AK_{17}[@i_{183}], mAK_{18}[@i_{183}], m, e5)$;
new $Nt_{192} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{192}\rangle$
$\oplus$ $@i_{182} \leq N$ **suchthat defined**$(x_{176}[@i_{182}], e4[@i_{182}], n[@i_{182}], ht[@i_{182}], AK_{17}[@i_{182}], mAK_{18}[@i_{182}]) \wedge ((m2 = e4[@i_{182}]) \wedge$ check2$(e4[@i_{182}],$ mkgen2$(rmKc), mac2))$ **then**
if $(Nc = n[@i_{182}])$ **then**
if $(h = ht[@i_{182}])$ **then**
new $r1_{193} : seed$;

new $ts_{194} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{194}), AK_{17}[@i_{182}], r1_{193})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{182}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{182}], mAK_{18}[@i_{182}], m, e5)$;
new $Nt_{195} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{195}\rangle$
$\oplus$ $@i_{181} \leq N$ **suchthat defined**$(x_{177}[@i_{181}], e4[@i_{181}], n[@i_{181}], ht[@i_{181}], AK_{17}[@i_{181}], mAK_{18}[@i_{181}]) \wedge ((m2 = e4[@i_{181}]) \wedge \mathsf{check2}(e4[@i_{181}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
if $(Nc = n[@i_{181}])$ **then**
if $(h = ht[@i_{181}])$ **then**
new $r1_{196} : seed$;
new $ts_{197} : timest$;
let $e5 : maxmac = \mathsf{enc}(\mathsf{pad}(\mathsf{C}, ts_{197}), AK_{17}[@i_{181}], r1_{196})$ **in**
let $mac5 : macs = \mathsf{mac}(e5, mAK_{18}[@i_{181}])$ **in**
event $\mathsf{partCT}(h, AK_{17}[@i_{181}], mAK_{18}[@i_{181}], m, e5)$;
new $Nt_{198} : nonce$;
$\overline{c4[!_{11}]}\langle m, mac1, e5, mac5, Nt_{198}\rangle$
$\oplus$ $@i_{180} \leq N$ **suchthat defined**$(x_{178}[@i_{180}], e3[@i_{180}]) \wedge ((m2 = e3[@i_{180}]) \wedge \mathsf{check2}(e3[@i_{180}], \mathsf{mkgen2}(rmKc), mac2))$ **then**
$\overline{0}$

|

$!^{!_{12} \leq N}$
$c14[!_{12}](hc : host, ht : host, n : nonce)$;
find $j1 \leq N2$ **suchthat defined**$(Rmkey_{28}[j1], Khost[j1], Kkey[j1], Kmkey[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2], Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{31} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{31})$ **in**
new $rmAK_{32} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{32})$ **in**
new $r3_{33} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{33})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{34} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{34})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{35} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{35})$ **in**
new $rmAK_{36} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{36})$ **in**
new $r3_{37} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{37})$ **in**
let $x_{67} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{38} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{38})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**

new $rAK_{39} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{39})$ **in**
new $rmAK_{40} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{40})$ **in**
new $r3_{41} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{41})$ **in**
let $x_{173} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{42} : seed$;
let $e4 : maxmac = \mathsf{enc}(\mathsf{concat1}(AK_{17}, mAK_{18}, n, ht), Kkey[j1], r4_{42})$ **in**
let $mac4 : macs = \mathsf{mac}(e4, Kmkey[j1])$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{29}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2],$
$Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{43} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{43})$ **in**
new $rmAK_{44} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{44})$ **in**
new $r3_{45} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{45})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{46} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{46})$ **in**
let $x_{68} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] =$
$ht)$ **then**
new $rAK_{47} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{47})$ **in**
new $rmAK_{48} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{48})$ **in**
new $r3_{49} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{49})$ **in**
let $x_{70} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{50} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{50})$ **in**
let $x_{69} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{51} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{51})$ **in**
new $rmAK_{52} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{52})$ **in**
new $r3_{53} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{53})$ **in**
let $x_{174} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{54} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKt), r4_{54})$ **in**
let $x_{71} : maxmac = \mathsf{cst\_maxmac}$ **in**

let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKt))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j1 \leq N2$ **suchthat defined**$(Rmkey_{30}[j1], Khost[j1]) \wedge (Khost[j1] = hc)$ **then**
find $j2 \leq N2$ **suchthat defined**$(Rmkey_{28}[j2], Khost[j2], Kkey[j2],$
$Kmkey[j2]) \wedge (Khost[j2] = ht)$ **then**
new $rAK_{55} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{55})$ **in**
new $rmAK_{56} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{56})$ **in**
new $r3_{57} : seed$;
let $e3 : maxmac = \mathsf{enc}(\mathsf{concat2}(AK_{17}, mAK_{18}, hc), Kkey[j2], r3_{57})$ **in**
let $mac3 : macs = \mathsf{mac}(e3, Kmkey[j2])$ **in**
new $r4_{58} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{58})$ **in**
let $x_{175} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{29}[j2], Khost[j2]) \wedge (Khost[j2] =$
$ht)$ **then**
new $rAK_{59} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{59})$ **in**
new $rmAK_{60} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{60})$ **in**
new $r3_{61} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKt), r3_{61})$ **in**
let $x_{72} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKt))$ **in**
new $r4_{62} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{62})$ **in**
let $x_{176} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
$\oplus$ $j2 \leq N2$ **suchthat defined**$(Rmkey_{30}[j2], Khost[j2]) \wedge (Khost[j2] =$
$ht)$ **then**
new $rAK_{63} : keyseed$;
let $AK_{17} : key = \mathsf{kgen}(rAK_{63})$ **in**
new $rmAK_{64} : mkeyseed$;
let $mAK_{18} : mkey = \mathsf{mkgen}(rmAK_{64})$ **in**
new $r3_{65} : seed$;
let $e3 : maxmac = \mathsf{enc2}(\mathsf{Zconcat2}, \mathsf{kgen2}(rKc), r3_{65})$ **in**
let $x_{178} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac3 : macs = \mathsf{mac2}(e3, \mathsf{mkgen2}(rmKc))$ **in**
new $r4_{66} : seed$;
let $e4 : maxmac = \mathsf{enc2}(\mathsf{Zconcat1}, \mathsf{kgen2}(rKc), r4_{66})$ **in**
let $x_{177} : maxmac = \mathsf{cst\_maxmac}$ **in**
let $mac4 : macs = \mathsf{mac2}(e4, \mathsf{mkgen2}(rmKc))$ **in**
$\overline{c15[!_{12}]}\langle hc, e3, mac3, e4, mac4\rangle$
|
$!^{!_{13} \leq N}$
$c7[!_{13}](m8 : maxmac, mac8 : macs, m9 : maxmac, mac9 : macs, n2 : nonce)$;
find $@i_{78} \leq N$ **suchthat defined**$(x_{67}[@i_{78}], e3[@i_{78}], mAK_{18}[@i_{78}], hc[@i_{78}], AK_{17}[@i_{78}]) \wedge ((m8 = e3[@i_{78}]) \wedge$
$\mathsf{check2}(e3[@i_{78}], \mathsf{mkgen2}(rmKt), mac8))$ **then**
if $\mathsf{check}(m9, mAK_{18}[@i_{78}], mac9)$ **then**
let $injbot(pad(= hc[@i_{78}], t : timest)) = \mathsf{dec}(m9, AK_{17}[@i_{78}])$ **in**

event partTC($hc[@i_{78}], AK_{17}[@i_{78}], mAK_{18}[@i_{78}], m8, m9$);
$\overline{c8[!_{13}]}\langle$acceptT($hc[@i_{78}]$)$\rangle$
$\oplus$ $@i_{77} \leq N$ **suchthat defined**($x_{68}[@i_{77}], e4[@i_{77}]$) $\wedge$ (($m8 = e4[@i_{77}]$) $\wedge$ check2($e4[@i_{77}]$, mkgen2($rmKt$), $mac8$)) **then**
$\overline{0}$
$\oplus$ $@i_{76} \leq N$ **suchthat defined**($x_{69}[@i_{76}], e4[@i_{76}]$) $\wedge$ (($m8 = e4[@i_{76}]$) $\wedge$ check2($e4[@i_{76}]$, mkgen2($rmKt$), $mac8$)) **then**
$\overline{0}$
$\oplus$ $@i_{75} \leq N$ **suchthat defined**($x_{70}[@i_{75}], e3[@i_{75}], mAK_{18}[@i_{75}], hc[@i_{75}], AK_{17}[@i_{75}]$) $\wedge$ (($m8 = e3[@i_{75}]$)$\wedge$
check2($e3[@i_{75}]$, mkgen2($rmKt$), $mac8$)) **then**
if check($m9, mAK_{18}[@i_{75}], mac9$) **then**
let $injbot(pad(= hc[@i_{75}], t : timest)) =$ dec($m9, AK_{17}[@i_{75}]$) **in**
event partTC($hc[@i_{75}], AK_{17}[@i_{75}], mAK_{18}[@i_{75}], m8, m9$);
$\overline{c8[!_{13}]}\langle$acceptT($hc[@i_{75}]$)$\rangle$
$\oplus$ $@i_{74} \leq N$ **suchthat defined**($x_{71}[@i_{74}], e4[@i_{74}]$) $\wedge$ (($m8 = e4[@i_{74}]$) $\wedge$ check2($e4[@i_{74}]$, mkgen2($rmKt$), $mac8$)) **then**
$\overline{0}$
$\oplus$ $@i_{73} \leq N$ **suchthat defined**($x_{72}[@i_{73}], e3[@i_{73}], mAK_{18}[@i_{73}], hc[@i_{73}], AK_{17}[@i_{73}]$) $\wedge$ (($m8 = e3[@i_{73}]$)$\wedge$
check2($e3[@i_{73}]$, mkgen2($rmKt$), $mac8$)) **then**
if check($m9, mAK_{18}[@i_{73}], mac9$) **then**
let $injbot(pad(= hc[@i_{73}], t : timest)) =$ dec($m9, AK_{17}[@i_{73}]$) **in**
event partTC($hc[@i_{73}], AK_{17}[@i_{73}], mAK_{18}[@i_{73}], m8, m9$);
$\overline{c8[!_{13}]}\langle$acceptT($hc[@i_{73}]$)$\rangle$
|
$!^{!_{14} \leq N2}$
$c13[!_{14}](Khost : host, Kkey : key, Kmkey : mkey)$;
if ($Khost =$ C) **then**
let $Rmkey_{30} : mkey =$ cst_mkey
else
if ($Khost =$ T) **then**
let $Rmkey_{29} : mkey =$ cst_mkey
else
let $Rmkey_{28} : mkey =$ cst_mkey
)

RESULT **time**(*context for game* 9) = **time**(C) $\times$ $N2$ + **time**(T) $\times$ $N2$ + 2. $\times$ **time**($=host$) $\times$ $N2$ + **time**(**let** concat2) $\times$ N + 2. $\times$ **time**(check) $\times$ N + 3. $\times$ **time**($=host$) $\times$ N + **time**(**let** pad) $\times$ N + 3. $\times$ **time**(**let** injbot) $\times$ N + 3. $\times$ **time**(dec) $\times$ N + **time**(acceptT) $\times$ N + **time**(kgen) $\times$ N + **time**(mkgen) $\times$ N + **time**(concat2) $\times$ N + **time**(concat1) $\times$ N + 3. $\times$ **time**(enc) $\times$ N + 3. $\times$ **time**(mac) $\times$ N + 6. $\times$ $N2$ $\times$ **time**($=host$) $\times$ N + **time**($=nonce$) $\times$ N + **time**(**let** concat1) $\times$ N + 3. $\times$ **time**(C) $\times$ N + **time**(pad) $\times$ N + 2. $\times$ **time**(kgen) + **time**(mkgen)
RESULT **time**(*context for game* 14) = **time**(C) $\times$ $N2$ + **time**(T) $\times$ $N2$ + 2. $\times$ **time**($=host$) $\times$ $N2$ + **time**(check) $\times$ N + 3. $\times$ **time**($=host$) $\times$ N + **time**(**let** pad) $\times$ N + 2. $\times$ **time**(**let** injbot) $\times$ N + 2. $\times$ **time**(dec) $\times$ N + **time**(acceptT) $\times$ N + 6. $\times$ N $\times$ N $\times$ **time**(check2) + 6. $\times$ N $\times$ N $\times$ **time**(mkgen2) + 6. $\times$ N $\times$ N $\times$ **time**($=maxmac$) + 3. $\times$ **time**(mac) $\times$ N + 2. $\times$ **time**(mkgen2) $\times$ N + 2. $\times$ **time**(mac2) $\times$ N + **time**(kgen) $\times$ N + **time**(mkgen) $\times$ N + **time**(concat2) $\times$ N + **time**(concat1) $\times$ N + 3. $\times$ **time**(enc) $\times$ N + 6. $\times$ $N2$ $\times$ **time**($=host$) $\times$ N + **time**($=nonce$) $\times$ N + **time**(**let** concat1) $\times$ N + 3. $\times$ **time**(C) $\times$ N + **time**(pad) $\times$ N + 2. $\times$ **time**(kgen)
RESULT **time**(*context for game* 21) = **time**(C) $\times$ $N2$ + **time**(T) $\times$ $N2$ + 2. $\times$ **time**($=host$) $\times$ $N2$ + **time**(check) $\times$ N + 3. $\times$ **time**($=host$) $\times$ N + **time**(**let** pad) $\times$ N + **time**(**let** injbot) $\times$ N + **time**(dec) $\times$ N + **time**(acceptT) $\times$ N + 12. $\times$ N $\times$ N $\times$ **time**(check2) + 12. $\times$ N $\times$ N $\times$ **time**(mkgen2) + 12. $\times$ N $\times$ N $\times$ **time**($=maxmac$) + 3. $\times$ **time**(mac) $\times$ N + 3. $\times$ **time**(enc) $\times$ N + **time**(kgen) $\times$ N + **time**(mkgen) $\times$ N + **time**(concat2) $\times$ N + **time**(concat1) $\times$ N + 2. $\times$ **time**(mkgen2) $\times$ N + 2. $\times$ **time**(mac2) $\times$ N + 6. $\times$ $N2$ $\times$ **time**($=host$) $\times$ N + **time**($=nonce$) $\times$ N + 3. $\times$ **time**(C) $\times$ N + **time**(pad) $\times$ N + **time**(kgen)
RESULT **time**(*context for game* 26) = **time**(C) $\times$ $N2$ + **time**(T) $\times$ $N2$ + 2. $\times$ **time**($=host$) $\times$ $N2$ + **time**(check) $\times$ N + 3. $\times$ **time**($=host$) $\times$ N + **time**(**let** pad) $\times$ N + **time**(**let** injbot) $\times$ N + **time**(dec) $\times$ N + **time**(acceptT) $\times$ N + 12. $\times$ N $\times$ N $\times$ **time**(check2) + 12. $\times$ N $\times$ N $\times$ **time**(mkgen2) + 12. $\times$ N $\times$ N $\times$ **time**($=maxmac$) + **time**(concat1) $\times$ N + 3. $\times$ **time**(enc) $\times$ N + 3. $\times$ **time**(mac) $\times$ N + **time**(concat2) $\times$ N + **time**(kgen) $\times$ N + **time**(mkgen) $\times$ N + **time**(Zconcat2) $\times$ N + **time**(Zconcat1) $\times$ N + 2. $\times$ **time**(kgen2) $\times$ N + 2. $\times$ **time**(enc2) $\times$ N + 2. $\times$ **time**(mkgen2) $\times$ N +

$2. \times \mathbf{time}(\mathsf{mac2}) \times N + 6. \times N2 \times \mathbf{time}(=host) \times N + \mathbf{time}(=nonce) \times N + 3. \times \mathbf{time}(\mathsf{C}) \times N +$
$\mathbf{time}(\mathsf{pad}) \times N$
Could not prove event $\mathsf{partTC}(\mathsf{C}, k, mk, x, y) \Longrightarrow \mathsf{partCT}(\mathsf{T}, k, mk, x', y)$.
n