$\{\text{"HELLO"}, n_A^{\#1}\}_{SK(A)}\}, \{(1, f, \emptyset), [recv_2, claim_3]\}\}$

$\rightarrow \langle\langle \{A, B, pK(A), pK(B), \{\text{"HELLO"}, n_A^{\#1}\}_{SK(A)}\}, \{(1, f, \emptyset), [recv_2, claim_3]\}\} \cup$
$\cup \{(2, f, \emptyset), running(P, r)\}\rangle\rangle \longrightarrow \dots$

ÎNCEP CU $\Delta_0(P)$. RULEZ PAȘII TRACE-ULUI ONEST (DEASUPRA SĂGEȚILOR SUNT FIX PAȘII, DAR SCRIȘI CU "i" ȘI "r"). APLIC REGULA PASULUI ("create", "send", "recv" → DIN CURSURI). CÂND TREC LA UN PAS NOU, ÎL SCOT DIN DREAPTA "→".

c) $\gamma = claim_\ell(R, recent\text{-}alive, R')$ deducă

$(\forall) \mathcal{t} \in traces(P) \wedge (\forall)(\theta, f, \nabla) \in Just_{\mathcal{t}}$ a.î. $((\theta, f, \nabla), \gamma) \in \mathcal{t}$
$\wedge honest(\theta, f, \nabla)$, atunci:

$(\exists) ev, ev' \in \mathcal{t}$ a.î. $actor(ev) = f(R') \wedge role(ev) = R' \wedge$
$running(ev') = running(\theta, f, \nabla) \wedge ev' <_t ev <_t ((\theta, f, \nabla), \gamma)$

FIE $\mathcal{t} \in traces(P)$, FIE $(\theta, f, \nabla) \in Just_{\mathcal{t}}$ a.î. $((\theta, f, \nabla), \gamma) \in \mathcal{t}$
$\wedge honest(\theta, f, \nabla)$:

$ev' = send_1$
$ev = send_2$
$\gamma = claim_3(i, recent\text{-}alive, r)$

} RESPECTĂ PROPRIETĂȚILE, DECI $(\exists)$

q.e.d

Seminar 8 (Model Examen)

1) SĂ SE DEM. "$f \to \psi$" PLECÂND DE LA O MULȚIME "T" DE ASUMPȚII.

$T \cup \{f\} \vdash \psi$

(a) $i \models S \sim X$
(b) $i \models \#(X)$
(c) $i \models S \models X$
(d) $i \models S \Rightarrow X$
(e) $i \models X$

$$\frac{\{S \sim X\} \cup A_\Gamma}{(\exists) i : i \models X}$$

$$\frac{i \models j \sim nu \quad i \models \#(nu)}{i \models j \models nu}$$

$$\frac{i \models j \models nu \quad i \models j \Rightarrow nu}{i \models nu}$$

2) FIE PROTOCOLUL "P": $i \to r : i, r$

$r \to i : \{r, n_r\}_{pk(i)}$

$i \to r : \{n_r, i\}_{pk(r)}$

a) $P(i), P(r) = ?$

FIIND "f" FIXAT, $f = \{i \mapsto A, r \mapsto B\}$; $runsof(P, i), runsof(P, r) = ?$

b) SĂ SE EXEMPLIFICE UN ATAC.

c) SĂ SE SCRIE UN TRACE ONEST ȘI SĂ SE EXECUTE "n" PAȘI ÎN SEMANTICA OPERAȚIONALĂ.

d) SĂ SE VERIFICE DACĂ URMĂTORUL "claim" E VALID:

$\gamma = claim_4(r, recent\text{-}alive\text{-}correct\text{-}role, i)$

a) $\mathbb{N}^{\#} = \mathbb{N}$

$P(i) = \{\{i, r, sk(i), pk(i), pk(r)\}, [send_1(i, r, (i, r)), recv_2(i, r, \{r, V\}_{pk(i)}), send_3(i, r, \{V, i\}_{pk(r)})]\}$

$P(r) = \{\{i, r, sk(r), pk(i), pk(r)\}, [recv_1(r, i, (i, r)), send_2(r, i, \{r, n_r\}_{pk(i)}), recv_3(r, i, \{n_r, i\}_{pk(r)}), claim_4(r, recent\text{-}alive\text{-}correct\text{-}role, i)]\}$

$runsof(P, i) = \{((1, f, \emptyset), [send_1(A, B, (A, B)), recv_2(A, B, \{B, V\}_{pk(A)}), send_3(A, B, \{V, A\}_{pk(B)})])\}$

$runsof(P, r) = \{((2, f, \emptyset), [recv_1(B, A, (A, B)), send_2(B, A, \{B, n_B^{\#2}\}_{pk(A)}), recv_3(B, A, \{n_B^{\#2}, A\}_{pk(B)}), claim_4(B, r\text{-}a\text{-}c\text{-}r, A)])\}$

c) TRACE ONEST "P": $[\overbrace{((1, f, \emptyset), create(i))}^{PAS1}, \overbrace{((1, f, \emptyset), send_1(A, B, (A, B)))}^{PAS2}, ((2, f, \emptyset), create(r)), ((2, f, \emptyset), recv_1(B, A, (A, B))), ((2, f, \emptyset), send_2(B, A, \{B, n_B^{\#2}\}_{pk(A)})), ((1, f, \{V \to n_B^{\#2}\}), recv_2(A, B, \{B, V\}_{pk(A)})), ((1, f, \{V \to n_B^{\#2}\}), send_3(A, B, \{V, A\}_{pk(B)})), ((2, f, \emptyset), recv_3(B, A, \{n_B^{\#2}, A\}_{pk(B)})), ((2, f, \emptyset), claim_4(\dots))]$

STARE INIȚIALĂ $= S_0(P) = \ll AKN_0, \emptyset \gg$; $AKN_0 = \{A, B, pk(A), pk(B)\}$

EXECUȚIE ÎN LTS: $\ll \{A, B, pk(A), pk(B)\}, \emptyset \gg \xrightarrow{PAS1} \ll \{A, B, pk(A), pk(B)\}, \{((1, f, \emptyset), [send_1, recv_2, send_3])\} \xrightarrow{PAS2} \ll \{A, B, pk(A), pk(B), (A, B)\}$

$\{((1, \mathcal{P}, \bar{\mathcal{Q}}), [recv_2, send_3])\}$ »

$i \to r : i, r$

$r \to i : \{r, n_r\}_{SK(r)}$

$i \to r : \{n_r, i\}_{SK(i)}$

$AKN_3 = \{A, B, pK(A), pK(B), (A,B), \{B, n_B^{\#2}\}_{SK(A)}\}$

$AKN_3^* = \{t \in AKN_3\} \cup \{t \mid AKN_3 \vdash t\}$

$AKN_3 \cup$ " — " "

$AKN_3 \vdash \{B, n_B^{\#2}\}_{SK(B)}$

$AKN_3 \vdash pK(B)$

$AKN_3 \vdash (B, n_B^{\#2})$

$AKN_3 \vdash n_B^{\#2}$

d) RECENT-ALIVE-IN-CORRECT-ROLE:

$(\forall)\, t \in traces(P) \wedge (\forall)\, inst : (inst, \gamma) \in t \wedge honest(inst) \Rightarrow$

$\Rightarrow (\exists)\, ev \in t : actor(ev) = \langle inst \rangle(i) \wedge \boxed{role(ev) = i} \wedge (\exists)\, ev' :$

↳ "IN-CORRECT-ROLE"

$: runid of(ev') = runid of(inst) \wedge ev' <_t ev <_t (inst, \gamma)$